INTELLIGENCE FUSION FOR COMBINED OPERATIONS

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

JOHN P. RITCHEY II, MAJ, USA
B.S., The Citadel, Charleston, South Carolina, 1980

Fort Leavenworth, Kansas
1994

Approved for public release; distribution is unlimited.

(1)

REPORT DOCUMENTATION PAGE

1. AGENCY USE ONLY

3 June 1994

Master's Thesis, 2 Aug 93-3 Jun 94

4. TITLE AND SUBTITLE

Intelligence Fusion for Combined Operations

6. AUTHOR(S)

Major John P. Ritchey II, USA

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

U.S. Army Command and General Staff College
ATTN: ATZL-SWD-GD
Fort Leavenworth, Kansas 66027-6900

9. SPONSORING MONITORING AGENCY NAME(S) AND ADDRESS(ES)

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION AVAILABILITY STATEMENT

Approved for public release, distribution is unlimited.

13. ABSTRACT (Maximum 200 words)

The. U.S. Army and the national intelligence community are undergoing revolutionary changes in the way intelligence is gathered, processed, and disseminated. The introduction of automation into the U.S. military has brought the modern battlefield into the information age, driving the operational commander's quest for certainty and expectations for intelligence information to new heights. As we anticipate fighting the next war, we will require a system that shares a common picture of the battlefield with all commanders. When dealing with intelligence, we often find a huge information gap between the capabilities of the U.S. forces and those of our potential allies. This study investigates the requirements of a multinational intelligence fusion system for the force projection Army of the future. This thesis researches the current and emerging doctrine on intelligence in combined operations, the lessons learned from the most recent combined operations, the current state of intelligence fusion capabilities, and the C4I for the Warrior concept as the potential solution to meet the requirements of intelligence fusion for combined operations. The study concludes with a basic endorsement of the intelligence fusion concept envisioned in C4I for the Warrior. Current intelligence information systems, such as Linked Operations-Intelligence Centers Europe (LOCE), provide the baseline for intelligence for combined operations.

14. SUBJECT TERMS

Joint Defense Intelligence Support Service (JDISS),
Linked Operations Intelligence Centers Europe (LOCE),
Fusion, Combined Intelligence

17. SECURITY CLASSIFICATION OF REPORT | 18. SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED UNCLASSIFIED UNCLASSIFIED

GENERAL INSTRUCTIONS FOR COMPLETING SF 298

The R[illegible] used [illegible] s important that th[illegible] page [illegible] to meet [illegible]

INTELLIGENCE FUSION FOR COMBINED OPERATIONS

A thesis presented to the Faculty of the U.S. Army
Command and General Staff College in partial
fulfillment of the requirements for the
degree

MASTER OF MILITARY ART AND SCIENCE

by

JOHN P. RITCHEY II, MAJ, USA
B.S., The Citadel, Charleston, South Carolina, 1980

Fort Leavenworth, Kansas
1994

MASTER OF MILITARY ART AND SCIENCE

THESIS APPROVAL PAGE

Name of candidate: Major John P. Ritchey II

Title of thesis: Intelligence Fusion for Combined Operations

Approved by:

Michael E. Barrington, Thesis Committee Chairman
Lt Col Michael E. Barrington, B.S.

, Member
LTC Kathleen R. Sower, B.A.

, Member, Consulting Faculty
LTC Ernest M. Pitt, Jr., J.D.

Accepted this 3rd day of June 1994 by:

Philip J. Brookes, Director, Graduate Degree Programs
Philip J. Brookes, Ph.D.

The opinions and conclusion expressed herein are those of the student author and do not necessarily represent the views of the U.S. Army Command and General Staff College or any other government agency. (References to this study should include the foregoing statement.)

ABSTRACT

INTELLIGENCE FUSION FOR COMBINED OPERATIONS by Major John P. Ritchey II, USA, 99 pages.

The U.S. Army and the national intelligence community are undergoing revolutionary changes in the way intelligence is gathered, processed, and disseminated. The introduction of automation into the U.S. military has brought the modern battlefield into the information age, driving the operational commander's quest for certainty and expectations for intelligence information to new heights. As we anticipate fighting the next war, we will require a system that shares with all commanders a common picture of the battlefield.

When dealing with intelligence, we often find a huge information gap between the capabilities of the U.S. forces and our potential allies. This study investigates the requirements of a multinational intelligence fusion system for the force projection Army of the future. This thesis researches the current and emerging doctrine on intelligence in combined operations, the lessons learned from the most recent combined operations, the current state of intelligence fusion capabilities, and the C4I for the Warrior concept as the potential solution to meet the requirements of intelligence fusion for combined operations. The study concludes with a basic endorsement of the intelligence fusion concept envisioned in C4I for the Warrior with current intelligence information systems, such as Linked Operations-Intelligence Centers Europe (LOCE), as the baseline.

TABLE OF CONTENTS

Page

LIST OF ILLUSTRATIONS

LIST OF ABBREVIATIONS

AIA - Army Intelligence Agency

AFCEA - Armed Forces Communications and Electronics Association

AFCENT - Headquarters Allied Forces Central Europe

ARCENT - Army Central Command; also U.S. Third Army

ASAS - All Source Analysis System

ATCCS - Army Tactical Command and Control System

AUTODIN - Automatic Digital Network

AWACS - Airborne Warning and Control System

BICES - Battlefield Information Collection and Exploitation System

CGSC - Command and General Staff College

CI - Counter-Intelligence

CIA - Central Intelligence Agency

COA - Course of Action

COMINT - Communications Intelligence

CONUS - Continental United States

CORCEN - Correlation Center

COTS - Commercial Off-The-Shelf

CR-CCIS - Central Region Command and Control Information System

C3I - Command, Control, Communications, and Intelligence

C4I -Command, Control, Communications, Computers, and Intelligence

DIA - Defense Intelligence Agency

DISN - Defense Integrated Secure Network

DISA - Defense Information Systems Agency

DISE - Deployable Intelligence Support Element

DoD - Department of Defense

DoDIIS - Department of Defense Intelligence Information System

EAC - Echelons Above Corps

ECB - Echelons Corps and Below

ENSCE - Enemy Situation Correlation Element

ELINT - Electronics Intelligence

FAS - Feasibility, Acceptability, Suitability

FLCS - Force Level Control System

HUMINT - Human Intelligence

IEW - Intelligence Electronic Warfare

IMINT - Imagery Intelligence

IPB - Intelligence Preparation of the Battlefield

IRDB - Individual Reports Database

ISE - Intelligence Support Element

JASMIN - Joint Analysis System for Military Intelligence

JIC - Joint Intelligence Center

JDISS - Joint Defense Intelligence Support Services

JSTARS - Joint Surveillance Target Attack Radar System

JTFPMO - Joint Tactical Fusion Program Office

JTIDS - Joint Tactical Information Distribution System

JUDI - Joint Universal Data Interpreter

LAN - Local Area Network

LANTCOM - Atlantic Command

LOCE - Linked Operations-Intelligence Centers Europe

METT-T - Mission, Enemy, Troops available, Terrain, and Time

MIIDS - Military Intelligence Integrated Data Systems

NATO - North Atlantic Treaty Organization

NSA - National Security Agency

NESEA - Naval Electronics Systems Engineering Activity

NGO - Non-Governmental Organization

NTCS-A - Naval Tactical Command System- Afloat

PC - Personal Computer

QSTAG - Quadripartite Standard Agreements

RTS - Remote Terminal Servers

SAM - Strategic Assessment Module

SATCOM - Sattelite Communications

SCI - Sensitive Compartmented Information

SHAPE - Supreme Headquarters Allied Powers Europe

SIDS - Secondary Imagery Dissemination System

SIGINT - Signals Intelligence

STANAG - Standard NATO Agreement

STACCS - Standard Theater Army Command and Control System

TENCAP - Tactical Exploitation of National Capabilities

THMT - Tactical High Mobility Terminal

TOC - Tactical Operations Center

UAV - Unmanned Aerial Vehicle

UNITAF - Unified Task Force

USACOM - U. S. Atlantic Command

USEUCOM - U.S. European Command

USMTF - U.S. Message Text Formats

CHAPTER 1

INTRODUCTION

The U.S. Army and the national intelligence community are undergoing revolutionary changes in the way intelligence is gathered, processed, and disseminated. The introduction of automation into the U.S. military has brought the modern battlefield into the information age, driving the operational commander's quest for certainty and expectations for intelligence information to new heights. This new increase in capability affords the operational commander and the intelligence community the ability to store and retrieve vast amounts of data. Lightweight satellite communications and packet switching have added another dimension to the ease in which the U.S. military can move and exchange information around the battlefield. This expansive reservoir of data, however, is of limited use if it does not provide timely, relevant information to military commanders. Tne power of our computers must be harnessed to provide us useful, militarily significant information in the form of a "fused" product - not only national, but also multinational. The U.S. armed forces will not fight unilaterally on the next battlefield. As we anticipate fighting the next war, we will require a system that shares a common picture of the battlefield with all commanders. When processing intelligence information, we find a huge information gap between the capabilities of the U.S. forces and those of our potential military allies. The need for fused intelligence, shared with coalition partners, is widely recognized and accepted at all levels, but little effort has been expended to develop a system which truly shares intelligence information with coalition partners. This study will identify the requirements of a multinational intelligence system for the force projection Army of the future. It will look at the current state of intelligence fusion systems in the U.S. Army, in Joint commands, and in combined organizations, and address whether these existing systems can fulfill the requirement of multinational forces.

Combined operations have been a reality of the American military since the birth of the nation. From the siege of Yorktown during the American Revolution to Desert Storm, the American military has combined efforts with other nations. The 1992 national military strategy and the new Army warfighting doctrine emphasize a requirement not only to fight jointly but also to fight as part of combined (multinational) military operations. The latest national defense strategy is based on four key foundations: Strategic Deterrence and Defense, Forward Presence, Crisis Response, and Reconstitution. It changes from a policy designed to contain communism, to a more flexible strategy directed toward regional rather than global threats. This new direction will require innovative thinking and a fresh look into the command and control of multinational forces. Key to the success of the new national defense strategy will be the automated command and control of the battlefield and the electronic systems required to aid commanders in their decision making. A principal part of the decision making process is the intelligence which commanders receive at all levels. Too much intelligence, however, is often worse than not enough. A careful balance must be reached through the use of automated intelligence fusion techniques.

During the past twenty years the U.S. military has devoted an enormous effort toward the development of automated command and control and intelligence fusion capabilities for "U.S. only" organizations. The rapid advancement of automated information systems has given the U.S. military the edge in technology and with it the capability to share quickly and efficiently information over extended distances. However, future wars will not be fought unilaterally and the allied forces will not necessarily be sophisticated organizations. Should we begin now to develop an intelligence fusion system which is multifunctional, multinational, and deployable upon demand to any corner of the world? Should not a future system provide the basics of modern intelligence doctrine, provide a common picture of the battlefield, and support IEW synchronization and targeting? The questions are all relative and retorical.

The new FM 100-5, Operations, recognizes an Army of change. The 1993 doctrine reflects the Army in a strategic era in which a force projection Army can build and sustain substantial combat power in remote regions of the globe, an era in which "operations outside the United States will usually be in conjunction with allies." [1] During future conflicts, much will depend upon the initial planning and performance of our armed forces and the forces of our allies. Quick victory with minimum casualties is the expectation of our nation. Proper staff planning and information sharing at all levels and across all boundaries, to include multinational boundaries, will be key to the initial success of the next confrontation. A "common intelligence picture of the battlefield," one in which information is shared vertically as well as horizontally, will be required for all commanders - not just U.S. commanders.

Since the conduct of unilateral military operations in the future is questionable, an entire chapter of the new 100-5 has been devoted to combined operations. This document recognizes the challenges that the U.S. Army faces when conducting military operations with allied or coalition partners. It underscores the requirement for commanders to fully understand the true capabilities of their counterparts. It recognizes that "most allies cannot approach the range of US capabilities to collect and process intelligence" [2] and that intelligence collection, production, and dissemination are major challenges. The process of disseminating operational and tactical military intelligence to allied and coalition forces is almost totally through liaison officers and the formation of a combined intelligence staff developed at theater level. Past experience shows that this method is slow and cumbersome. True integration of the combined intelligence requirements and display of a common picture lend themselves to automated fusion.

Purpose of the Thesis

The importance of this thesis is to research the current doctrine on combined operations, to define the current state of intelligence fusion capabilities, to determine how they fit into current command and control structures, and to suggest how they can be applied toward developing an objective architecture capable of supporting combined operations. **The thesis question focuses on what kind of system we should use to exchange intelligence data with coalition partners in a force projection army.**

As the primary question focuses on identifying the requirements for a computer system which will assist in providing a common picture of the battlefield to our allies, a number of subordinate questions unfold. The major secondary questions posed by the research question are as follows: What is the current doctrine as it applies to intelligence in combined operations? What are the current intelligence information systems available? What is "adequate" in terms of intelligence support to the commander in a combined or allied environment? What is the appropriate command level for a multinational system? Some tertiary questions include: What is the current status of prototype systems? What form should a future system take? What type of databases should we make available to our allies? How will we manage these databases? Can we provide near-real-time information to allied nations (ELINT, IMINT)? What type of intelligence information does the United States expect in return? What type of communications system is required? How do we deal with the language differences? How do we accomplish multilevel security? When so many levels of concern must be addressed, there are no simple answers to the many complex questions.

Background

The fall of the Berlin Wall and the subsequent breakup of the Soviet Union symbolized the beginning of the end of the communist ideology and of a power which, despite its defects, helped to maintain world stability.[3] The fall of this ideology appears to have eliminated any likelihood of a global war, but at the same time the instability resulting from the dramatic shift has increased the likelihood of lessor regional conflict throughout Europe and what is known as the Commonwealth of Independent States (CIS). There are essentially new rules for maintaining world order now that the constraints of the bipolar world are removed and there is a new set of players. Europe, for example, is not just forty-eight recognized states, but we must now acknowledge the viability of

160 ethnic groups, all seeking to establish their roles and positions. Although the threat of direct large scale conventional military confrontation in Europe appears to have greatly diminished, the regional turmoil this "New World Order" has created is compelling the United States to relook its warfighting philosophy - from the strategic to the tactical level. As a result, the United States has modified its National Security Strategy to demonstrate its resolve as a world leader in promoting peace throughout the world.

In order to understand the impact of the national strategy, a look at the current world situation reveals where the United States may be required to serve as a leader in regional stability. In Europe, the United States has an interest in promoting peace throughout the region and maintains a vital interest in the control of nuclear weapons and arms proliferation in the former Soviet Union.[4] In Asia, the United States maintains a military presence in support of stable North-South Korea relations and promotes positive change in China, Laos, and Cambodia. In the Middle East and South Asia, the United States maintains forces in the region to defend the sovereignty, independence, and territorial integrity of its partners in the region.[5] Finally, in Latin America, the United States pledges to advocate multinational responses to aggression, to participate in peacekeeping operations, arms control, and the undertaking of major counter-drug, counter-terrorism and nation assistance missions. In light of the instability and potential commitment of forces that now exists in virtually every corner of the globe, the U.S. Army faces an unprecedented challenge of preparing for multiple contigency requirements, some of which may be impossible to predict. As the world becomes more unstable, our military is also downsizing. National intelligence organizations which once monitored every corner of the globe are reducing their staffs commensurate with the rest of the Department of Defense. The harsh reality is that we no longer will enjoy the luxury of a teams of analysts devoted to every country in the world. In fact, it is highly likely that many potential adversaries will go unmonitored by U.S. intelligence analysts. The U.S. will be forced to rely to some extent on the intelligence services of our allies and the practice of shared intelligence will become more routine.

The subject of shared intelligence is not unknown and several prototype systems have been and will be developed and tested. In an attempt to focus the scope of this thesis, NATO will serve as the primary example for future capabilities. Because of the current state of the new world order, the European theater offers a chance to view forces of a mature multinational theater which may commit to out-of-area operations.

In order to meet the anticipated intelligence requirements of NATO during an armed conflict with the former Soviet Union, a testbed system was developed in Europe during the early 1980's under the proponency of USEUCOM. The system is called Linked Ops-Intel Centers Europe (LOCE) and it was intended to be both a joint and combined intelligence fusion system. MG John Stewart, Commandant, U.S. Army Intelligence Center and School and G2 of ARCENT during the Gulf War, said, during a recent visit to the Command and General Staff College, that the concept of providing intelligence to allied nations through a system such as LOCE is a concept worth exploring. His briefing slides portrayed a mobile "LOCE type" intelligence system capable of future deployments anywhere in the USEUCOM area of operations.

We shall address NATO for a number of significant reasons. "Planning will become more complex as the Soviet 'threat' recedes and new risks emerge from the breakup of the Soviet Union." [6] First, the U.S. has pledged a commitment to NATO and continues to support NATO with military forces, to include participation in the new multinational corps organization under development. Secondly, there are and will continue to be significant threats or "risks" to the member states of NATO. Preserving its vitality serves the interests of the member states and the interests of Europe and the rest of the world. Finally, NATO states have economic, security, and other reasons to be concerned about instability outside the NATO area. Under the new strategic conditions, NATO confronts significantly reduced levels of risk in the Central Region but maintains a significant risk on the flanks. Southeastern Europe, Southwest Asia, and the eastern Mediterranean littorals are the greatest risks, particularly Greece and Turkey. Only under the umbrella of NATO can European and U.S. forces effectively train and prepare for combined out-of-area operations. The forces most likely to deploy will be the newly created Rapid Reaction Force, commanded by a British officer, of which the U.S. has committed a significant membership. In this event, U.S. forces could conceivably be commanded by a foreign officer with potentially limited intelligence capabilities.

Key to the development of any combined intelligence system is the opinion and the cooperation of the other nations involved. This becomes particularly important as we look for the *quid pro quo* in the maintenance of an intelligence database. Within NATO, Supreme Headquarters Allied Powers Europe (SHAPE) has taken the lead in the identification of requirements for a future NATO system called Battlefield Information Collection and Exploitation System (BICES). BICES "will link the battlefield intelligence systems of individual NATO countries and relay critical battlefield information...to the division commander on the European battlefield." [7]

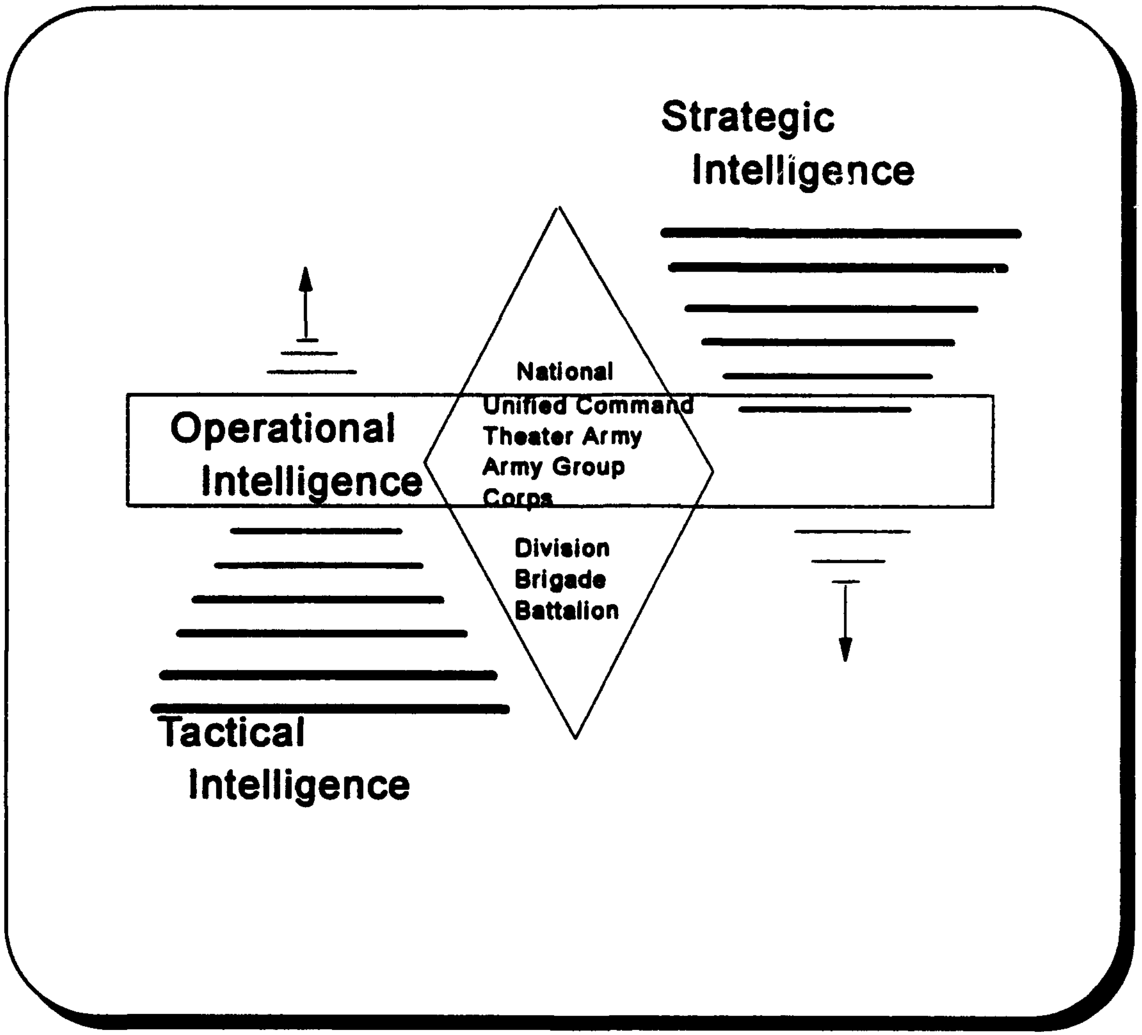


Fig. 1. Operational Intelligence Relationship to Tactical and Strategic Intelligence.
Source: U.S. Army, FM 34-1, Intelligence and Electronic Warfare Operations, (Washington, D.C.: U.S.GPO, 1987), 2-9.

As the current status of intelligence fusion systems in NATO is reviewed, the parallel system development of purely national systems within the intelligence community must be understood. A good understanding of what systems are available at the strategic, operational, and tactical levels within the U.S. military intelligence community and of how the flow of intelligence will be accomplished in the future is vital to determining a direction in combined operations. Additionally, in almost all military operations, the intelligence production effort has been purely a national responsibility. In view of this historical precedent, the logical place to interface the tactical intelligence requirements with the national intelligence capabilities is at the operational level.

Each service has its own intelligence system designed to meet the needs of the tactical community in development or in operation. The intelligence system of the future at the tactical level for the U.S. Army is the All Source Analysis System (ASAS). From corps to brigade, ASAS terminals will provide the common situational display. At the operational level, each unified commander has his own project under development. The newly formed USACOM will use the system developed under LANTCOM called Joint Defense Intelligence Support Services (JDISS). JDISS links the tactical intelligence community with the strategic data bases within national agencies. The link to combined agencies is not as clear and proves to be a significant obstacle during any armed conflict in which the U.S. participates as a coalition partner.

During the Gulf War it became increasingly obvious to combat commanders that the U.S. did not have a well defined, robust command and control or intelligence communication architecture in place. Although the technology was available in a variety of commercial off-the-shelf capabilities, our Army ran on the relatively unsophisticated personal computer (PC). Additionally, during the initial stages of the war, no national strategy harnessed the technological capabilities of the systems available. In March

1992, General Colin Powell, then Chairman, Joint Chiefs of Staff, briefed the Senate Armed Services Committee on a new program called C4I for the Warrior. He explained that under this new concept, we were reviewing the communications and intelligence systems purchased for the future to ensure interoperability. VADM Macke, Joint Staff J6, described this new approach as fulfilling the warrior's needs for "a fused, real time, true representation of the warrior's battlespace - an ability to order, respond, and coordinate horizontally and vertically to the degree necessary to prosecute his mission in that battlespace." [8] This new concept appears to be an intelligence system of systems with an objective architecture not to be reached well into the year 2010. The concept calls for the integration of intelligence fusion as well as multinational interoperability.

A number of problems can be anticipated with developing a multinational approach to intelligence as evidenced by our slow acceptance of the current joint doctrine. Numerous problems will be realized with the evolving combined intelligence doctrine, the interoperability of systems and the training of allied nations on intelligence fundamentals. Lt Col W.E. Wickam, USMC, a scholar from the Naval War College, wrote the following about intelligence in the joint environment:

> U. S. military successes in Panama and in the Persian Gulf have validated the concept of jointness legislated by the Goldwater-Nichols Act. Service and joint operational doctrine now express similar themes. Implicit in joint operational doctrine is the necessity to integrate operations and intelligence. However, the need for operational intelligence has not yet been fully embraced in the joint environment for three reasons. First, there is a lack of good joint intelligence doctrine. Second, the organization of U.S. military intelligence has historically evolved along service lines. This factor has also hindered the

> development of interoperable intelligence systems. Third, joint intelligence training is rare because of the lack of a doctrinal and organizational base.[9]

Many of the same problems we are experiencing with integrating joint operations and intelligence will probably apply to combined operations with the additional barriers of language and culture. First among those is the lack of a published doctrine that addresses combined operations at the operational level of war. Joint Pub 2-0, Doctrine for Intelligence Support to Joint Operations, was just signed in September 1993. It provides the basis for joint intelligence doctrine of the future. FM 100-8 Combined Army Operations (Preliminary Draft), January 1992, is the Army's first attempt at providing the Army perspective of combined operations. These manuals as well as Joint Pub 3-0, Doctrine for Unified and Joint Operations will begin to fill the void. Next is that with the exception of NATO and Korea, we have relatively limited experience sharing intelligence information via automated information systems with multinational forces. A paticularly difficult problem results when we engage in a coalition with military forces which have little or no computer background or capability. Lastly, the age old challenge of security and releasability of U.S. intelligence information to foreign militaries remains the achilles heal when attempting to form combined intelligence centers and share intelligence information. Creating a true common picture of the battlefield will not be completely accomplished until our allies can reap the benefits of the power of the U.S. intelligence community as they fight by our side.

Assumptions

Four assumptions need to be taken into account as the thesis is developed. Firstly it must be assumed that the United States will fight any future conflict in concert with allied or coalition forces. The allied or coalition force will create a combined headquarters and intelligence information will be required to support the combined staff. Secondly, we will assume that there is a requirement for intelligence "fusion" in combined operations and that the national intelligence community will develop a stated requirement for the development of a separate system which will interface with allied and coalition forces. Thirdly, we must assume that in a relatively short period of time the U.S. national intelligence community will develop a multilevel security system which will meet the joint and combined needs. The future capability would include the screening and filtering of information to retain its true intelligence content and not be skewed in accuracy to an extent that it would be useless to our allied or coalition partners. Lastly, we will assume that we would use the same system (hardware and software) across the operational continuum. It would support high intensity conflict as well as operations other than war, and such a system could meet the needs of military actions involving a graduated response, such as the current Somalia relief effort.

Limitations

Because many of the documents related to ASAS, LOCE, and JDISS are classified, certain limitations exist when developing the thesis. The basic text of this thesis will remain unclassified. Consequently, technical details and characteristics will not be discussed. Also, much of the text will use NATO as an example for future development of systems in support of regional CINC's. Although much of the documentation is unclassified, many NATO documents are NATO Restricted, which causes the research to restrict the data to

USEUCOM information and may prejudice some of the outcome toward a more U.S. point-of-view. This thesis will not address all intelligence systems developed by every service at every level. The thesis will be limited to examining a few of the systems which have made significant contributions to joint and combined operations as they pertain to the land component operation. In order to further reduce the scope, we shall focus primarily on the operational level of war in which "joint and combined operational forces within a theater of operations perform subordinate campaigns and major operations ... to accomplish the strategic objectives of the unified commander or higher military authority."[10]

Definition of Terms

In order to limit the scope of the thesis and to eliminate any ambiguities we must define key terms which will be useful in clarifying and understanding the problem. For the limited scope of this thesis, the following definitions apply:

Battlespace as defined by C4I for the Warrior:

> The Warrior's Battlespace is any area over which the Warrior exercises control or has a military interest. Commanders require an integrated picture of the ground, air, maritime, space, and special operations being conducted in the Battlespace. [11]

Fusion as defined by the Joint Chiefs of Staff in "C4I for the Warrior" :

> Fusion is the process of receiving and integrating all-source, multi-media and multi-format information to produce and make available an accurate, complete summary that is timely, but more concise, less redundant, and more useful to the warrior than if the same information were received directly from separate multiple sources.[12]

Interoperability as defined by JCS Pub 1-02 :

> Interoperability is the ability of systems, units, or forces to provide services to and to accept services from other systems,

> units or forces, and to use the exchanged services to operate effectively together. [13]

Operational Intelligence as defined by FM 34-1:

> That intelligence which is required for the planning and conduct of campaigns within a theater of war. At the operational level of war, intelligence concentrates on the collection, identification, location, and analysis of strategic and operational centers of gravity. If successfully attacked, they will achieve friendly political and military-strategic objectives within a theater of war. [14]

Finally, it is important to understand combined command structures. Coalitions and alliances are the result of nations combining military forces. "Coalitions are ad hoc arrangements between two or more nations for a common action." [15] They are normally developed for a short period of time, are usually formed as a rapid response to an unforeseen crisis, and are customarily less structured than an alliance. "Alliances are, typically, the result of formal agreements between two or more nations for broad, long-term objectives." [16] Many considerations must be observed when entering into a combined operation. As we complete the transition from peacetime competition to conflict and war, the sharing of intelligence will become critical.

Significance of the Study

This thesis should assist the Army to better understand the options available and the potential requirement for a specific intelligence fusion system designed especially for combined operations. Despite any conclusions drawn from this study, an endorsement for an emphasis on the continued development of intelligence fusion systems will be provided. Whether current systems can fulfill the requirement or whether a new architecture is required is not as important as the recognition of the overall need for interoperability and intelligence fusion capabilities with the militaries of our allies.

Endnotes

[1] U.S. Army, FM 100-5, Operations, (Washington, D.C.: U.S. GPO 1993), iv.

[2] Ibid., 5-4.

[3] U.S. Army, Office of the Deputy Chief of Staff for Operations and Plans, State of America's Army, (Washington, D.C.: U.S. GPO 1993), 1.

[4] The White House, United States of America National Security Strategy, (Washington, D.C.: US GPO, January 1993), 7.

[5] Ibid., 20.

[6] Ted Greenwood and Stuart Johnson, "NATO Force Planning Without the Soviet Threat," C320 Corps and Division Operations (Ft Leavenworth, KS: US GPO, August 1993), 2-25.

[7] Daniel J. Marcus, "NATO Plans Major Review of Intelligence System," Army Times (February 1988): 34.

[8] Joint Chief of Staff Pamphlet, "C4I for the Warrior," (Washington, D.C.:U.S. GPO, 1992), 3.

[9] W.E. Wickam, "Institutionalizing Operational Intelligence in the Joint Environment." (Rhode Island: Naval War College, 1992), ii.

[10] FM 100-5, 6-2.

[11] C4I for the Warrior, 9.

[12] Ibid., 13.

[13] Ibid., 2.

[14] FM 34-1, 2-10.

[15] U.S. Army, FM 100-8, Combined Army Operations (Preliminary Draft), (Washington, D.C.: U.S. GPO, 1992), 2-5.

[16] Ibid.

CHAPTER 2

REVIEW OF THE LITERATURE

Command, Control, Communications, and Intelligence (C4I) is beginning to attract much attention, particularly as it relates to joint and combined operations. Several documents address this latest of trends in the U.S. military. The most pertinent exists in the form of national military strategy and in articles written by the Joint and Army staff which address the future of warfare and C4I for the Warrior.

Fundamental to the thesis question will be whether there exists a requirement for a combined (*multinational*) intelligence fusion system. Although this is a fundamental assumption, the answer evolved from the research of the current and emerging doctrine as well as from the basic intelligence deficiencies of past wars. Information from books, magazine articles, documents from the Center for Army Lessons Learned on the Gulf War, and reports to Congress reveal insight into intelligence related lessons learned and into potential solutions. Also, each of the services conducts a requirements study prior to dedicating resources to the development of information systems. These documents are available from the program director's test and evaluation agencies. A review of these documents gives the history and points to the expected future of these systems.

Conducting research on a contemporary topic generally restricts the literature for review. Thus, only the most recent literature can be used as background information. Of considerable importance are the views of senior officers attending the war college. Consequently, the review of theses prepared by war college students is critical. Additionally, School for Advanced Military Science (SAMS) students as well as Command and General Staff College students have written relevant research papers. The opinions and critical thought of these contemporary writers provide unique insight into operational intelligence as well as automated command and control techniques.

Doctrine drives the way we fight. Consequently, understanding the emerging doctrine is of primary importance to the thesis. Much of the latest in doctrine was just recently published within the past year. Two key Joint manuals, Joint Pub 2-0, Doctrine for Intelligence Support to Joint Operations and Joint Pub 3-0, Doctrine for Unified and Joint Operations , identify the common service intelligence functions and the ends toward which the intelligence community must collectively work. They provide not only the J-2's perspective of intelligence but also the commander's perspective of the uses of intelligence information. Since these are the first manuals in the military hierarchy to discuss intelligence for combined operations, we will use the principles of intelligence quality as the criteria for the basic characteristics of intelligence in support of combined operations in the remainder of our study. Additionally, FM 100-5, the Army's primary warfighting manual, was recently released. As can be expected, with the change in the Army's capstone manual comes changes to the intelligence doctrine in the form of FM 34-1, Intelligence and Electronic Warfare, currently under revision. With the added emphasis of our new doctrine on coalition warfare comes a new manual, FM 100-8, Combined Army Operations, currently in a preliminary draft stage.

These key manuals provide the foundation for intelligence requirements in combined operations.

In response to the new military strategy and the emphasis placed on both joint and combined operations, the Joint Staff published several comprehensive information packets which describe the C4I for the Warrior concept. These packets, as well as *Military Review* articles on the subject, form the basis for the introduction of the C4I for the Warrior concept into the thesis. The study of this concept gives us an understanding of the degree to which an intelligence architecture is currently being planned.

Four books, all published by AFCEA International Press, the publishers of *Signal Magazine*, provide the best thinking as it relates to C4I in the Army, Navy, Marine Corps, Air Force, Joint Services, and other government agencies. These books give insight into C4I systems management and the challenges associated with information and technology transfer. Of particular significance is the most recent of these books, The First Information War, which provides outstanding insight into how information was used as a weapon and target during the Persian Gulf War. Published in October 1992, it is the most recent comprehensive collection of thoughts on how intelligence and information systems interacted during the war.

Professional military journals are a good source of unclassified up-to-date information on current doctrine, system development, and emerging technology. One of the best sources for evolving concepts and doctrine at the tactical and operational level is *Military Review*. This publication is invaluable in determining the latest schools of thought as we try to understand the realities of coalition warfare and the requirement for timely processed information. In it senior leaders routinely provide their thoughts on command, control, communications, computers, and intelligence (C4I).

After *Military Review*, probably the best professional magazine for understanding the changing roles of intelligence is *Military Intelligence*. It, frequently, expresses the latest views and concepts for deploying and employing Army forces in the future, and gives insight from MI professionals on how the intelligence system of systems can deliver strategic, operational, and tactical level intelligence to combat commanders. Of particular importance is the March 1993, *Military Intelligence* article titled "Intelligence Branch Operational Concept." This article describes the revolution in the way Army intelligence will support combat commanders, now and into the 21st century. This article is the professional military intelligence community's first look at the concept which the TRADOC Commander approved for strategic, operational, and tactical level intelligence support to commanders through the year 2002. This article, as well as the concept paper which supports it, will drive the future of the Army's intelligence doctrine in the form of a revised FM 34-1, Intelligence and Electronic Warfare Operations.

Signal and *International Defense Review*, two other journals, provide an abundance of technical and political background information for the development of information systems. Both give insight into the current state of C4I systems under development within and outside NATO; they also give insight to how systems are received by NATO; they give some insight into the progress of Standard Agreements (STANAGs) to define terminal and message requirements. Of particular interest is an *International Defense Review* article written by a British Army Officer, while serving as the Assistant Chief of Staff Intelligence at Headquarters Allied Forces Central Europe (AFCENT). This article gives a wider understanding of the BICES concept for inter-netting and fusing of NATO's intelligence systems. Other articles, as well as a chapter from the book Control of Joint Forces, by AFCEA, give a better understanding into integrating system architecture's and NATO interoperability.

Fundamental to the understanding of how the Army will be effected by intelligence fusion in multinational operations is the understanding of the Army Tactical Command and Control System (ATCCS) and the relationship of ASAS, the U.S. tactical intelligence system, to ATCCS. Since the early 1980's there have been numerous articles written in military journals on the development of ASAS - the concept, its capabilities, information management, and the communications required to support the system. The Program Executive Office of Army Tactical Command and Control Systems in Ft Hood, Texas, has been invaluable in providing information on the ATCCS system and the future integration of C2 systems. These documents develop the basic framework of an intelligence fusion systems capability with ASAS as the premiere intelligence system for the Army. *Military Intelligence* and *Signal* magazines are the main source of current information on the status of ATCCS and the interface of the ASAS system, as well as of the results of the 1993 Initial Operational Test and Evaluation (IOT&E) of ASAS.

For NATO, intelligence fusion is not a new concept. NATO and the U.S. European Command (USEUCOM) have been wrestling with the problem of sharing intelligence information through automated systems for years. USEUCOM documents from the Joint Analysis Center, LOCE Program Office, provide keen insight to chart the development of LOCE, to establish its origins, and to plot its direction. These documents clearly establish a basis for understanding a European perspective for a multinational architecture that is working now and has true growth potential to be a model for future multinational intelligence systems. Briefings acquired from the SHAPE intelligence staff show the acceptance of LOCE as the NATO gateway to BICES. A study of documents from the NATO Communication Information Service Agency (NACISA) and of open source articles from Allied Forces Central Region (AFCENT) gives insight into the NATO concept of BICES and shows LOCE's contribution to the BICES concept. Through articles from *Military Review*, *Military Technology*, and *Army Communications Magazine* the intelligence information systems reported to be developed by other nations will also be examined.

The availability of a specific requirements study identifying the need for a future intelligence fusion system designed for combined operations is missing from the documentation. The lack of this data and a specific requirements statement from the national intelligence community dictate an inductive methodology for the preparation of the thesis.

Interviews with Army intelligence officers involved in the most recent conflicts provide a personal accounting of the flow of intelligence from a user perspective. For example, one officer was assigned as an ARCENT liaison officer to a Saudi Arabian unit in the Gulf War and gave insight into the challenges associated with a high intensity conflict. In another case the officer was assigned as a brigade S2 during the initial phases of the operations in Somalia and gave insight into the particular problems associated with a conflict which began as a humanitarian effort and escalated into a peacemaking operation.

Overall, documentation of the various systems and historical data is generally available. However, quite a challenge remains to convince many sources to release the required information. Despite the lack of a specific requirements study supporting the development of a future intelligence fusion capability for combined operations, the amount of resource material is sufficient to draw documented conclusions and to continue with the analysis of the data.

CHAPTER 3

METHODOLOGY

The research methodology for this thesis combines descriptive, historical, and comparative analysis of the intelligence doctrine in support of combined operations and the computer information systems available to support that doctrine. The systems will be evaluated based on the criteria associated with the intelligence doctrine and the elements established by the U.S. Army CGSC Strategic Analysis Methodology (SAM). The conclusions will support intelligence fusion systems based on their feasibility, suitability, and acceptability.

The descriptive portion of the research focuses on the historical lessons learned, a review of the literature on emerging intelligence doctrine, and a discussion of the development of intelligence systems at each level of war - strategic, operational, and tactical. Several currently fielded common intelligence information systems will be examined to identify the current capabilities in support of the doctrine. C4I for the Warrior will then be examined as a conceptual answer for the future.

The historical portion will focus on the lessons learned of combined operations. A study of the two most recent conflicts involving the U.S. and coalition partners at the two extremes of the operational continuum will show the application of current automated intelligence systems and identify their deficiencies in support of doctrinal procedures. Desert Shield and Desert

Storm will be the example of a high intensity combat operation; Somalia will serve as an example of a low intensity conflict scenario.

The comparative portion will focus on the doctrine and the lessons learned. Within the doctrine exists a number of principles for intelligence quality and principles for joint intelligence operations which will be accepted criteria for combined operations. These principles will be the basis on which the current and proposed systems will be compared. This thesis will compare the doctrine with the lessons learned, will determine if any of the current systems are adequate, and will compare the results with the C4I for the Warrior concept of the future.

The final analysis of the evidence will focus on the feasibility, suitability, and acceptability (FAS) elements as established in the CGSC SAM, commonly referred to as the FAS test. The SAM provides a basic methodology for evaluating courses of action (COA) to determine if particular options will result in successful instruments of policy.[1] As a majority of the comparative evaluation will be subjective and many of the criteria are difficult to quantify, use of the SAM mechanism will lend credence to the final outcome. Each of the elements identified in the SAM will directly correspond to one or more of the major subordinate questions established in the thesis.

In the context of the SAM, feasibility centers on the current doctrine as it applies to intelligence in combined operations. Feasibility depends on the whether the action can be accomplished by the means available.[2] In the context of this thesis feasibility relates directly to whether or not the current intelligence systems available adhere to the doctrine. Do they meet the requirements identified by the principles of intelligence identified by joint and service manuals?

Suitability centers on the effectiveness of a particular course of action. Will it obtain the desired effect?[3] In this thesis suitability reflects what is "adequate" in terms of support to the modern commander in a combined environment. Is the operational level the appropriate level for a multinational system?

Acceptability centers on the concept of the ends justifying the means. Is the national will and the military leadership prepared to accept the chosen COA? "If the military objective is suitable and the military concept is feasible, the military means required must be cost effective."[4] In the context of this thesis, the ultimate aim is to evaluate if the Army's plans and systems to support those plans in combined operations is an acceptable solution to the modern commander.

Through the use of a methodology in which the evidence is presented in the form of a descriptive, comparative, and historical context and then evaluated based on criteria established by the CGSC SAM, the thesis question will be appropriately addressed. The use of the CGSC SAM will form the basis of the analysis of the data and the concluding chapter of this thesis.

Endnotes

[1] U.S. Army, C510 Syllabus, Joint and Combined Environments, (Ft Leavenworth, KS: U.S. GPO, 1993), 27.

[2] Ibid.,28.

[3] Ibid., 27.

[4] Ibid., 28.

CHAPTER 4

LESSONS LEARNED AND DOCTRINE

To examine fully the thesis question we must understand the evolution of our current intelligence system. With the development of today's sophisticated airborne and ground based collectors, the modern intelligence officer can be inundated with volumes of information. Generally this information is the product of national systems developed in support of strategic intelligence requirements. The proliferation of computers and satellite communications have allowed much of the strategic intelligence information, previously retained at the highest level, to now enter into the division tactical operations center (TOC). Because of the predominant multinational approach to warfighting, tactical intelligence officers are becoming dependent on strategic systems to support their collection requirements. This top down approach differs greatly from the traditional bottoms up system which has worked for centuries.[1] As we prepare to conduct force projection operations, intelligence will lack detail in the initial stages and tactical units will pull intelligence from national data bases. The key to the success of deploying forces will be the ability of national and theater intelligence assets to fulfill the tactical intelligence requirement.[2] A large part of that intelligence will be focused on information derived from host nation support and allied or coalition forces.

One of the primary assumptions of this thesis concerns a stated requirement for an intelligence fusion capability in combined operations. The basis for this assumption originates with the Goldwater-Nichols DoD Reorganization Act of 1986. This act set the stage for the current joint doctrine and the President's National Security Strategy and ultimately the National Military Strategy. The current National Military Strategy develops the premise that the warfighting focus will be taken away from global war and oriented toward regional threats vital to U.S interests. To build upon the National Defense Foundations, we shall employ a set of Strategic Principles which capitalize on our strengths. The principle of collective security cites "we expect to strengthen world response to crisis through multilateral operations under the auspices of international security organizations."[3] It continues to endorse the formal alliances, such as NATO, but underscores the requirement to fight as part of an ad hoc coalition, and to maintain the ability to fight as an independent force. Although intelligence operations are not specifically mentioned, other than maintaining a superior technological edge, clearly a requirement for the development of interoperable systems (operations, intelligence, etc.) at all levels (joint and combined) is implied.

Lessons Learned

In order to gain an appreciation for the complexities of intelligence in combined operations, and more importantly to explore what can be automated, we will briefly review the latest conflicts involving U.S. forces in combined operations. A look at the Gulf War will provide insight into a high intensity conflict in which we had months to conduct the build up and collect intelligence. A look at the Somalia operation will provide insight into a classic "operation other than war," which began as a humanitarian relief effort and escalated in to armed conflict in a low intensity scenario.

Lessons Learned in the Gulf War

The interim report to Congress on the conduct of the Persian Gulf War cites the overall intelligence support to Desert Shield and Desert Storm as successful. It heralds that no other commander in history had the capability to view his adversary as did our field commander, General H. Norman Schwarzkopf. "No other nation or coalition of nations has ever had the ability that the Coalition possessed during the Gulf crisis to collect information and disseminate intelligence."[4] The success of the Gulf War was contributed in high regard to the significant investment in technology, the ability to quickly correlate large amounts of data and to translate it into meaningful intelligence.

This conflict proved that the development of joint operations doctrine had surpassed the current intelligence doctrine. The primary lesson learned was that all services and government agencies must have compatible intelligence dissemination and communication systems. Although many field expedient fixes were developed, coping with the interoperability problems was often times at the expense of timeliness. Combined intelligence efforts were generally accepted as working well. Intelligence officers from the United Kingdom, Canada, and Australia all augmented the CENTCOM J-2 staff. The other coalition partners shared intelligence through a coordination center established in Riyadh, Saudi Arabia. The need to develop the Joint Intelligence Center (JIC), refine the doctrine, institutionalize the architecture, and exercise it routinely was a key component of the after action report.[5]

From the ARCENT perspective, MG Stewart, ARCENT G2, identified a number of challenges. The first was an organizational challenge. He needed to build an ARCENT G2 team and create an infrastructure for a new staff. A part of that challenge was the building of an IEW architecture which would enhance intelligence communications, computer, and collection capabilities. The linking of ARCENT with CENTCOM and the Army Intelligence Agency (AIA) as well as the integration of corps and divisions into that architecture was the cornerstone. This new architecture needed to be flexible and expandable. As it evolved, several major new systems, such as UAV, Joint STARS, and TROJAN SPIRIT, needed to be integrated.[6] " In Desert Storm, intelligence was real. It was a vital battlefield operating system."[7] A key component to the military intelligence success was the focus of intelligence downward. From the ARCENT view, that focus was from the corps down to the warfighters.

The immediate challenge to focusing the intelligence downward was working with a finite number of intelligence systems, limited further by the enemy's infrequent use of radios. For example, there was limited HUMINT until just before G-day. Consequently, the ARCENT staff relied heavily on imagery, which was constrained by the weather and the inherent limited capabilities of the imagery systems. Without much in between they could take blurred wide angle photos or very clear spot photos of a single point on the ground.

Connectivity was key. If the ARCENT staff could not get information from national sources and could not share intelligence with the corps, then it was functionally useless. They needed to provide connectivity to quickly receive requests for information and transmit responses (to include the transfer of digitized imagery). The answer was a connection to a communications and computer link, called Department of Defense Intelligence Information System (DoDIIS), directly into AIA. This allowed an on-line access to intelligence databases within AIA and DIA. Through DoDIIS high rates of imagery data were transfered from AIA to ARCENT. [8]

With a fairly robust net established to AIA, the next challenge was to establish a communication and computer network with the corps and divisions. Although tactical intelligence assets were deployed, many of the units were kept out of range from the collection targets until just before G-day. They were fed intelligence from the top down in order to conduct their planning. TROJAN SPIRIT (a digital and secure voice capability utilizing satellites) was deployed to the corps and most divisions. The Army Space Program Office deployed a Secondary Imagery Dissemination System (SIDS) to VII Corps as an imagery receive capability. The XVIII Airborne Corps used the organic Tactical High Mobility Terminal (THMT), a Tactical Exploitation of National Capabilities (TENCAP) system, as well as other systems to link with Ft Bragg for digital imagery and other support. This robust network of systems was planned and executed within just a few short months. Much of the hardware was commercial off-the-shelf equipment.

Although Joint STARS was not at full operational capability during the Gulf War, its contributions were significant. MG Stewart said, "Joint STARS was the single most valuable intelligence collection and targeting system in Desert Storm."[9] It is claimed to have contributed to every priority intelligence requirement during the ground war. Although it was not the single source of intelligence, Joint STARS was certainly instrumental in developing the intelligence picture of the battlefield. The current doctrine calls for Joint STARS ground station modules for corps and divisions.

Another significant concern was the limited availability of linguists. Two factors impacted on the availability of linguists. Foremost was the inherent difficulty for Americans to learn Arabic and secondly was that the Army requirement for Arabic linguists was less than for other languages. This caused a shortfall in the number of linguists available for intelligence functions, let alone civil affairs and interpreters. Reserve component Arabic speakers and Kuwaitis filled the void. Another major contributor to the overall successful effort was the exchange of liaison officers. These liaison elements provided an invaluable service in exchanging intelligence and maintaining open lines of communication between higher, lower, and adjacent units.

Lessons Learned from Somalia

MG Anthony C. Zinni, Director of Operations, Unified Task Force (UNITAF), recently addressed a number of intelligence related successes and failures he saw during the five months he spent in Somalia as the Chief of Operations and later as a special staff officer assigned to Ambassador Oakley. One of the immediate concerns to his staff as the situation matured was preparing for the addition and reception of almost twenty-four coalition partners who wanted to participate in the initial "relief " effort. As the situation developed and it became obvious the U.N. had no plan to relieve the U.S. Task Force staff, the mission began to change. Initially, it transitioned to disarmament, then to refugee resettlement. After UNISOM took over, the mission became a quest to capture the ever elusive General Aideed, the number one warlord in the country.[10]

Through all of the mission changes and the frustrations associated with working with Non-Governmental Organization (NGO) workers came a confused intelligence picture. The intelligence situational display was disjointed at the national, tactical and operational levels. MG Zinni illustrated his frustration when he referred to the confusion as an "intel menu" where the commander could pick the enemy situation of choice since every intelligence agency shared a different viewpoint. In fact, not one single organization was pulling it all together and painting a common picture.[11]

MG Zinni was critical of the intelligence situation in Somalia. From the entire affair he garnered three major lessons learned. First was what he termed "cultural intelligence" disparity. As the military assumes more and more responisibility for Operations Other Than War (OOTW), the commander must have a firm appreciation for the cultural differences, language barriers, tribal hierarchies, medical problems, political sensitivities, etc. Second is the realization that the American military has an innate desire to have an enemy. Where there is no enemy, as in most humanitarian relief efforts, there will almost always be an intense desire to make one. General Adeed was never an enemy from a military perspective but became a political enemy from the U.N. perspective. The last problem was what he termed "mission creep." The task force commander accepted a mission, but once on the ground the mission continued to change. MG Zinni could not stress enough the importance of the political leadership having a clear aim prior to the commitment of military forces. The resulting confusion ended in ineffective units and potential political and military embarrassment, as well as in the loss of life.[12]

When asked to explain the intelligence shortfalls in more detail, MG Zinni elaborated on the good as well as the bad. He felt that intelligence at the tactical level was extremely good. He lauded the efforts of the Counter-Intelligence (CI) and Human Intelligence (HUMINT) efforts, such as unit reconnaissance. He felt that the Operational Level Signals Intelligence (SIGINT) and Imagery gave him a reliable means of verifying what they were receiving from HUMINT sources. He believed that the analysts on the ground were doing some good synthesis of the data available and that their assessments were adequate.[13] However, what MG Zinni found particularly distressing was the distortion between the picture his intelligence officers were painting and the intelligence reports he read from the national or strategic intelligence community. The picture in Washington, where the political policy makers were located, was different from his picture. Even though he had strategic, operational, and tactical intelligence representatives all physically on the ground and contained within a relatively small area, there remained different pictures.[14]

Army intelligence personnel identified a number of problems with the integration of coalition partners into the intelligence operations. Among them was the problem of information exchange due to the incompatability of communications and computer equipment and the general lack of a data transfer capability. This forced units to dominate the operations nets with intelligence information. The 10th Mountain Division G2 recommended that communications equipment be procured to support coalition forces until their equipment arrived in country, similar to the way the USAF and USMC supported the U.S. Army initially.[15]

The 10th Mountain Division G2 pushed hard to receive the TROJAN SPIRIT system so they would have the ability to do split based operations and reduce the number of intelligence analysts required on the ground. Only five of these systems exist in the XVIII Airborne Corps. TROJAN SPIRIT proved to be a "versatile intelligence communications system with dedicated SATCOM, power generation and operations/ maintenance support [which] is ideal for contingency and/or planned deployments to an austere environment."[16] Although the system was primarily designed to support SIGINT operations, the Army's Hawkeye, LANTCOM's JDISS, and a number of other systems were tied into the TROJAN network to make it a responsive multifunctional special intelligence (SI) high communications and intelligence system. The G2 quickly realized that TROJAN SPIRIT was the most reliable means of communication between Somalia and the US.[17] This system allowed the 10th Mountain Division to conduct the initial test of a significant change to the emerging doctrine.

The Emerging Joint Intelligence Doctrine

The keystone manual for the joint intelligence doctrine is Joint Pub 2-0, initially scheduled for publication in September 1993 it is still a draft publication. The draft manual discusses principles for joint operations, responsibilities for joint operations, and intelligence for combined operations. The last chapter of Joint Pub 2-0, Intelligence for Combined Operations, specifies there can be "no single intelligence doctrine for combined operations."[18] It goes on to say that the principles of joint operations apply equally to combined operations. It specifies that "special arrangements" should be considered for "developing, communicating, and using intelligence information when there are differences in nations' culture, language and terminology, organizations, and structures, operating and intelligence concepts, methodologies and/or equipment."[40] Although this chapter never explains how to make these "special arrangements," it goes on to endorse the use of a Combined Intelligence Center, when there is a combined command, and the extensive use of liaison officers.

JCS Pub 2-0 recognizes three levels of intelligence: Strategic, Tactical, and Operational. Strategic intelligence has historically been considered that intelligence required for the formation of policy and plans at national and international levels. It deals almost exclusively with information generated by CIA, DIA, JCS, DoD, and the NCA. Tactical intelligence is recognized as that intelligence required for the conduct of operations at echelons corps and below. The terms tactical and strategic intelligence generally apply to the level of associated command. As we evolve into a more expeditionary force, the requirement for information from "national" intelligence producers becomes a requirement for tactical commanders. The requirement to share intelligence resources and manage those resources so they are properly focused and meet the requirements of a multitude of users is a universally recognized challenge.

In the quest to give decision makers enough information, we risk information overload by providing the commanders too much data. Massive quantities of information is of no value if it is not correlated and quantified. In an attempt to define the operational requirements for the intelligence staff, Joint Pub 2-0 (Test) published seven principles of intelligence quality to describe the attributes of intelligence for intelligence operations. They offer qualitative objectives for intelligence operations and establish a standard by which they can be evaluated. These same principles can be used to measure the capability of a current intelligence system or can form the basis of a future system's requirements document. The following are the principles of intelligence quality as outlined in Joint Pub 2-0 (Test):

PRINCIPLES OF INTELLIGENCE QUALITY

TIMELINESS: Intelligence must be available and accessible in time to effectively use it.

OBJECTIVITY : Intelligence must be unbiased, undistorted, and free from political influence or constraint.

USABILITY : The form in which intelligence is provided to the user must be suitable for application upon receipt without additional analysis.

READINESS : Intelligence must anticipate and be ready to respond to the existing and contingent intelligence requirements of commanders, staffs, and forces at all levels of command.

COMPLETENESS : Commanders, staffs, and forces must receive all the intelligence information they need to meet their responsibilities and accomplish their missions.

ACCURACY : Intelligence must be factually correct and convey the situation as it actually exists.

RELEVANCE : Intelligence must contribute to an understanding of the situation, to determining objectives that will accomplish the commander's purposes and intents, and to planning, conducting, and evaluating operations.[41]

This publication also addresses intelligence principles that allow the joint force commander to optimize his own force in supporting intelligence capabilities. Joint force commanders can enhance their overall unit "jointness" through the determination of intelligence objectives and through the establishment of a clear direction for the intelligence effort. Highlighted is the importance of interoperability of both procedures and information between intelligence and command and control systems. The following are the principles for Joint Intelligence as outlined in Joint Pub 2-0:

PRINCIPLES FOR JOINT INTELLIGENCE

Joint Force Commander Determines Direction of Intelligence
View the Enemy as Joint or Unified
Constitute a Joint Intelligence Staff
Ensure Mutual Support and Sharing
Make Organic Intelligence Capabilities Available to the Joint Force Commander
Pursue Interoperability[42]

Pursuing the principle of interoperability is of primary importance to this study. This document emphasizes the importance that intelligence systems, communications, concepts, products, and language must be interoperable in order for the intelligence organizations to effectively exchange and use intelligence information. The Joint Pub 2-0 (Test) identifies the three major challenges for interoperability as they relate to joint intelligence doctrine. These challenges are the interoperability of systems, interoperability of intelligence information and products, and finally language. Communications interoperability is the key factor common to these challenges.

Joint Pub 2-0 (Test) recognizes there can be no single intelligence doctrine for combined operations. It states that each coalition or alliance must develop its own doctrine. However, a number of analogies come from similar intelligence requirements. The principles, issues, and answers to combined operations will be similar to joint operations. In combined operations, the differences in culture, language, and national perspectives must be addressed to establish the doctrine. This document fully endorses the exchange of pertinent intelligence information to gain the clearest common understanding of the enemy. The combined intelligence principle of "special arrangements" is offered as a technique for solving unique problems associated with communications, language and terminology, operating and intelligence concepts, methodologies and equipment. The exchange of liaison officers is highlighted as the method for bridging the understanding between cultures, languages, terminology, and methodologies.[22]

When a combined command is formed, a combined intelligence center should be integrated into the organization. The combined intelligence center gives the combined commanders, Chief of Intelligence (C-2), a capability for developing requirements statements and for the fusion of the intelligence contributions of all the nations. The combined intelligence center is identified as the location where multinational intelligence officers would collocate to form a common combined intelligence picture. The importance of this concept to this study is idenitfication of the conceptual location where intelligence fusion should occur.

Combined Army Operations

FM 100-8, Combined Army Operations (Preliminary Draft), was distributed 29 January 1992 and is the initial step beyond FM 100-5, Operations, by the Army to integrate combined operations into the doctrine. This document, mostly historical in nature, addresses both parallel and unilateral command structures as part of a coalition and the common command structures of an alliance.

Although the organizational structure may be different, the major functions performed by combined operational forces for executing campaigns and major operations are similar. Like other Army operations, they need to be assessed based on Mission, Enemy, Troops Available, Terrain and Time (METT-T). There are no new specific principles applied to combined operations. The primary concerns of this document toward intelligence issues stem from "what intelligence information can be shared with allies and who makes the decision?"[23]

Clearly FM 100-8 is in its infancy and the doctrine is still evolving. A look at FM 34-1, Intelligence and Electronic Warfare , shows a better understanding of intelligence in combined operations. It states that the principles of combined operations are based on the principles applied to joint operations. Because two or more countries are involved, additional factors must be considered. It identifies eight considerations as a guide to overcoming the obstacles inherent in dealing with the diverse nature of allied forces and their doctrine, national prerogatives and other obstacles to a unified IEW effort.[24] The following principles are identified by FM 34-1 as a guide:

Principles for IEW in Combined Operations

Develop a Combined IEW System
Establish channels for the flow of IEW data
Establish standard procedures for IEW operations
Develop a secure, reliable communications capability
Ensure a linguist capability
Establish a liaison between allied IEW units
Establish a common data base including formats
Ensure interoperability of equipment[25]

Of particular interest to this study are thoughts on the development of the IEW structure, data base, and procedures. The development of the IEW structure for combined operations will be largely driven by the nature of the supported force and theater. Since each combined force will be unique, the

IEW system which supports it will need to be tailored. Fig 3-1 depicts a generic combined intelligence staff, from FM 100-18, which includes inputs from each service component as well as a multinational staff.

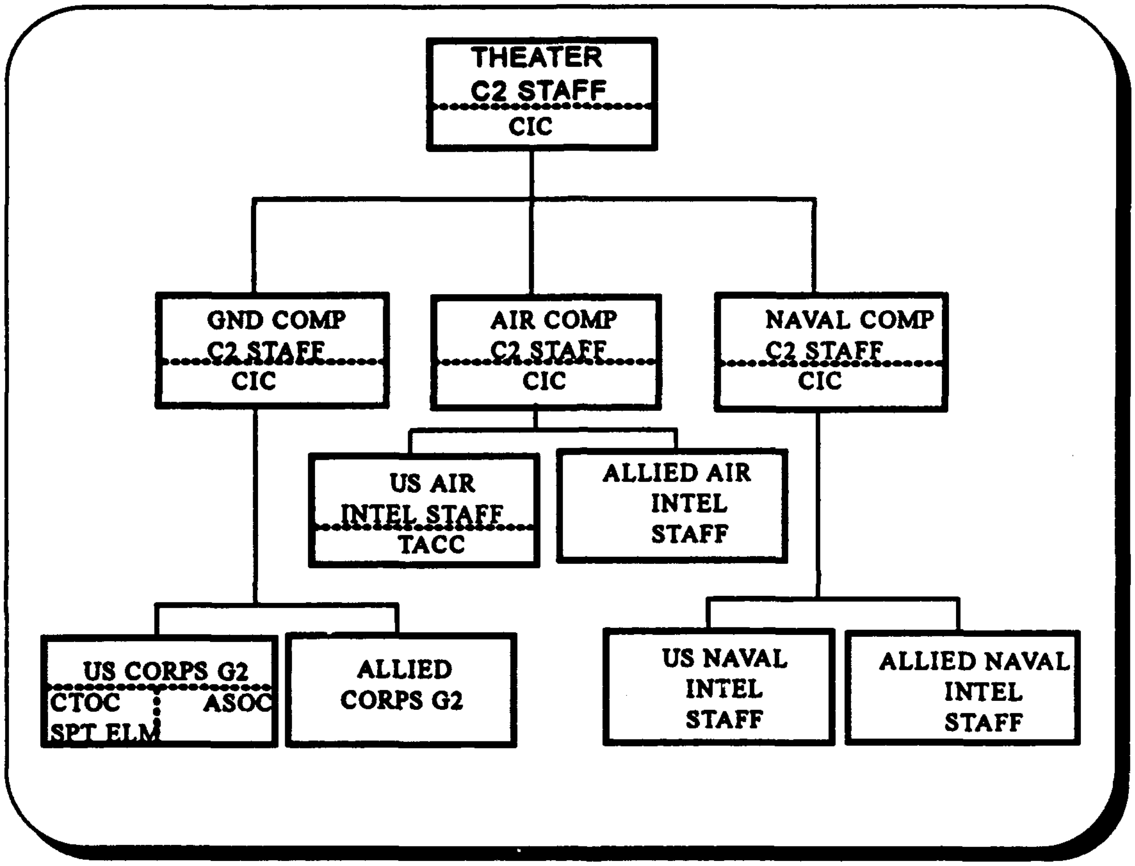


Fig. 2. Combined Intelligence Staff

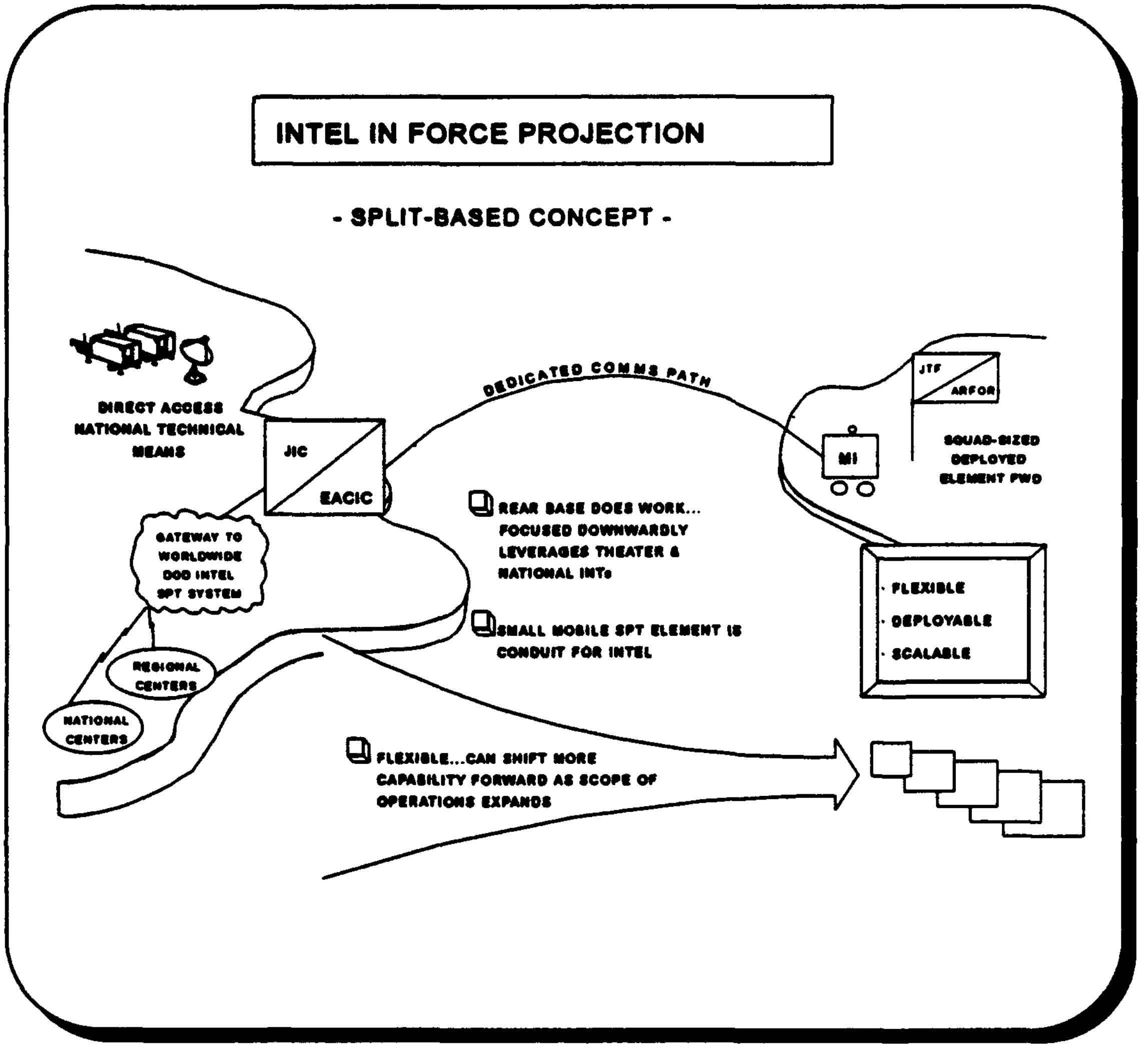
Source: U.S. Army, FM 34-1, Intellignce and Electronic Warfare Operations (Washington D.C.: US GPO, 1987), 13-9.

Releaseability of information to foreign militaries will be a major concern during the outbreak of hostilities. The underlying concept behind the development of a common picture can be hindered if the flow of information is impeded or blocked based on releaseability. Agreements concerning the exchange of information should be negotiated prior to hostilities when possible. Standard Agreements (STANAG) and Quadripartite Standard Agreements (QSTAG) are identified as examples of standard procedures which can be developed to assist the transition to war. Of particular importance is standardization of military terminology. When building computer databases, for example, the potential for double and triple reporting on the same entity is a reality.

This document emphasizes a need for the development of an intelligence data base as a combined effort during peace as a prelude to a quick and efficient transition to wartime intelligence operations. The data base should take an all source approach and should comply with national restrictions for the exchange of information. "Combined analysis based on IPB techniques will provide a common perspective of the threat and enhance a coordinated intelligence operation in case of war."[47]

Intelligence in Force Projection

Army intelligence forces and doctrine are evolving to support the new force requirements of the future. The requirement to project combat power from Continental United States (CONUS) bases will require the intelligence community to focus on a wide variety of regional threats. Echelons Above Corps (EAC) intelligence centers will continue to have a forward presence and be responsible for providing "processed" intelligence to operational and tactical echelons as well as providing "raw" intelligence data for intelligence processing. Echelons Corps and Below (ECB) will play a critical role once deployed for military operations. They will provide the detail and responsiveness to combat commanders to fight battles and engagements while still drawing information from EAC sources.



INTEL IN FORCE PROJECTION

- SPLIT-BASED CONCEPT -

❑ REAR BASE DOES WORK... FOCUSED DOWNWARDLY LEVERAGES THEATER & NATIONAL INTs

❑ SMALL MOBILE SPT ELEMENT IS CONDUIT FOR INTEL

❑ FLEXIBLE...CAN SHIFT MORE CAPABILITY FORWARD AS SCOPE OF OPERATIONS EXPANDS

DIRECT ACCESS NATIONAL TECHNICAL MEANS
JIC
EACIC
DEDICATED COMMS PATH
JTF
ARFOR
MI
SQUAD-SIZED DEPLOYED ELEMENT FWD
GATEWAY TO WORLDWIDE DOD INTEL SPT SYSTEM
REGIONAL CENTERS
NATIONAL CENTERS
· FLEXIBLE
· DEPLOYABLE
· SCALABLE

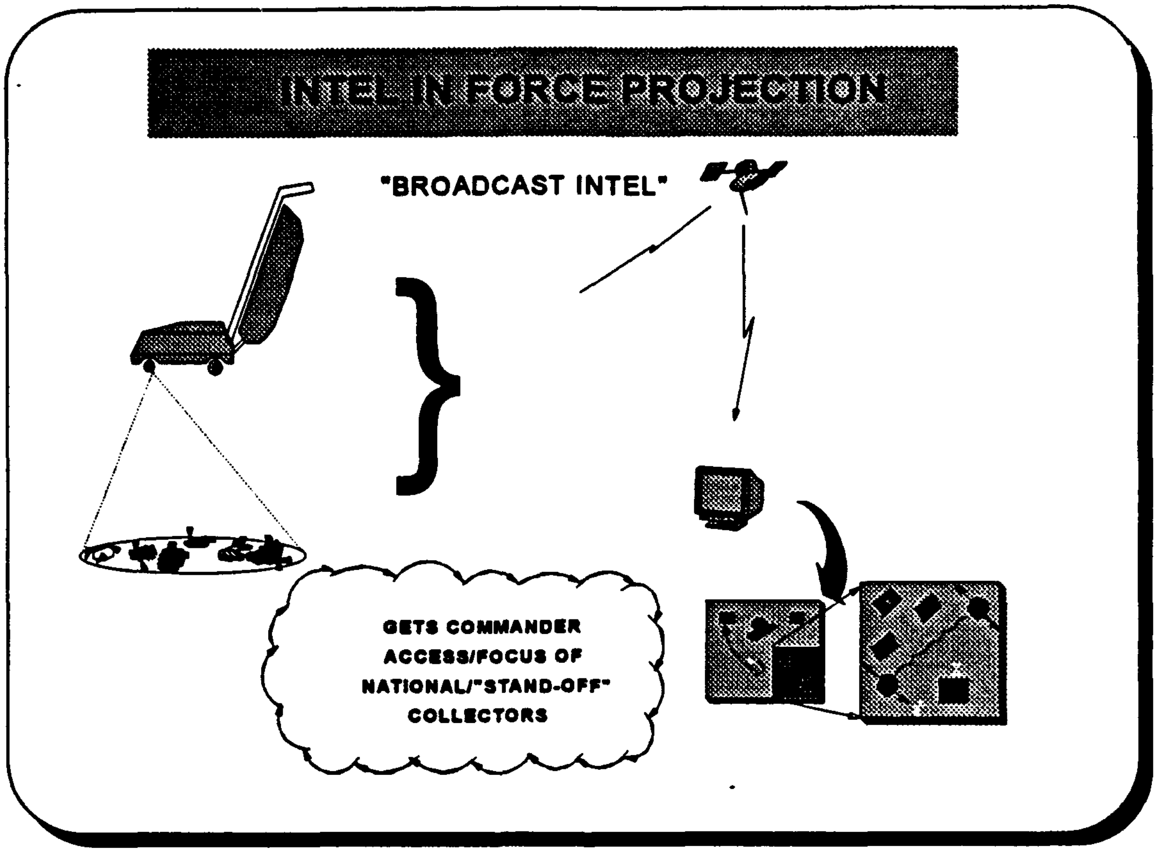
Fig. 3. Intelligence in Force Projection

Source: John F.Stewart, Jr. "MI Corps Intelligence Strategy - Intelligence in Force Projection." Briefing to CGSC intelligence officers, 4 August 1993, Ft Leavenworth, KS.

In order to support the largely CONUS based force, while adapting to a downsized force structure, a concept of split-based operation has emerged. It is driven by our doctrine. FM 100-5 necessitates that "key intelligence personnel and equipment must arrive in theater early."[48] The split-based concept centers around a forward intelligence team called a Deployable

Intelligence Support Element (DISE) which is tactically tailored according to the factors of METT-T, lift, and prepositioned assets. This team is either disbanded once the mission is accomplished or is the core, early-entry unit which is expanded as build-up operations are conducted. This tailored team receives its intelligence from an intelligence support base located in CONUS or outside the area of operations. This dynamic operations and intelligence approach integrates a split-based and a "broadcast" approach to intelligence support, in which the power of the national intelligence community can reach out to the forward commander who is actually doing the work. The concept allows a core set of rear based analysts to conduct the bulk of the intelligence analysis based on inputs from a variety of national and regional sources and provide "product" intelligence to a small mobile intelligence support team located forward with the combat force. The result is that the power of the national intelligence community is available to operational commanders with reduced numbers of intelligence staff requirements in the forward deployed headquarters.

This is a fundamental shift from the slow "pull" system of the past to a virtual vacuum cleaner style approach to acquiring sensor data in which the analyst is pulling from an established database which is virtually at one's fingertips in a matter of minutes. This split based concept depends on a common communications and intelligence processing capability at every echelon and requires a push system for intelligence support. The push support packages are based on Intelligence Support Elements (ISE) armed with computers and satellite communications (SATCOM) capability.



INTEL IN FORCE PROJECTION

"BROADCAST INTEL"

GETS COMMANDER ACCESS/FOCUS OF NATIONAL/"STAND-OFF" COLLECTORS

Fig. 4. Intelligence Support Element

Source: John F.Stewart, Jr. "MI Corps Intelligence Strategy - Intelligence in Force Projection." Briefing to CGSC intelligence officers, 4 August 1993, Ft Leavenworth, KS.

Endnotes

[1] Alan D. Campen, ed., "Communications Support to Intelligence," The First Information War, (Fairfax, VA: AFCEA International Press, 1992), 52.

[2] U.S. Army, FM 100-5, Operations (Washington, D.C.: US GPO, 1993), 3-3.

[3] Ibid, 8.

[4] Interim Report to Congress, July 1991, 14-1.

[5] Ibid.

[6] John F. Stewart, Jr., MG, USA "Desert Storm: A 3d Army Perspective," Military Intelligence, (Ft Huachuca, AZ: US GPO, October - December 1991), 22-23.

[7] Ibid., 23.

[8] Ibid., 24.

[9] Ibid., 29.

[10] MG Antony C. Zinni, USMC, address to the CGSC class on his view of Somalia, 30 November 1993, Ft Leavenworth, KS.

[11] Ibid.

[12] Ibid.

[13] Ibid

[14] Ibid.

[15] JULLS Report Number 12142-94679 (00108), Integration of Coalition Forces/Intelligence, submitted by G2, 10th Mtn Div, LTC Joyce, 22 March 1993.

[16] JULLS Report Number 10834-01832 (00104), Trojan Priorities and Requirements, submitted by G2, 10th Mtn Div, LTC Joyce, 22 March 1993.

[17] Ibid.

[18]Joint Pub 2-0 (Test Pub) Doctrine for Intelligence Support to Joint Operations (Washington, D.C.: U.S. GPO, June 1991), VI-1.

[19]Ibid, VI-2.

[20]Ibid, II-10.

[21]Ibid, II-30.

[22]Ibid, VI-2 - VI-4.

[23]FM 100-8, Combined Military Operations (Preliminary Draft), 2-17.

[24]FM 34-1, Intelligence and Electronic Warfare Operations, (Washington, D.C. :U.S. GPO, June 1987), 13-8.

[25]Ibid, 13-8.

[26]Ibid, 13-9.

[27]FM 100-5, 3-5.

CHAPTER 5

INTELLIGENCE FUSION SYSTEMS

The recent information explosion, the proliferation of the affordable PC within the military, and the slow development of a joint intelligence system have forced each service and each level of command to developed its own operations and intelligence computer architecture. Each command has spent enormous amounts of time, funding, and energy in the development of its own objective architecture. Attempts have also been made to connect with the evolving computer networks of our allies. Each of these systems has merit in its own right and we should not lose the lessons learned from their development. However, within the context of this study, only three of the most significant systems will be reviewed. The selection of these systems is the result of research which indicates these systems are most likely to be those which will survive in the future and will have potential input into combined operations through the land component commander. Since the enactment of the Goldwater-Nichols Act in 1986, the planners of computer networks have focused on integrating joint databases, on joint message formats, and on developing joint standards across the services. Within each requirements document, we also have detailed numerous requirements for integration in combined operations. However, there is no clear plan to integrate allies and coalition partners into our "infosphere." We will review three systems, one at each level of command and one acting as a U.S. gateway to a combined environment.

Joint Defense Intelligence Support Services

Joint Defense Intelligence Support Services (JDISS) is a system designed to provide Joint Intelligence Centers (JIC), Joint Task Forces(JTFs), and operational commanders with on-site automation and connectivity to support the intelligence mission. It is a core set of software running on a variety of different hardware platforms and using existing fixed-site as well as tactical communications systems. It is the technical baseline for the Department of Defense Intelligence Information System (DoDIIS) client-server environment and the foundation for future strategic to tactical interoperability. The intent is to use JDISS as a core product of DoDIIS to merge existing capabilities with off-the-shelf, commercially available products to satisfy the needs of Unified Commands, the Services and National Agencies.[1]

The executive agent for the JDISS program management is the Director of Naval Intelligence. A Joint Program Management Office has been established with staffing from all military services and DIA in Suitland, Maryland. The PMO manages the JDISS integration across DoD and ensures interoperability between JDISS and emerging service systems. It addresses system security accreditation, releasability and sanitization, and the integration of new functionalities for future software releases. [2]

The JDISS system has three main goals: provide single workstation access to intelligence databases to streamline deployed units, develope user interfaces which behave in a similar fashion regardless of the application or location, and ensure the interoperability of applications and data by rebuilding existing capabilities to accommodate the addition of future functionality. The JDISS program currently provides automated support to the following intelligence functions: "transmitting and receiving specific requests for intelligence; accessing theater, service and national intelligence databases; supporting digitized imagery exchange; accessing automated record message processing systems, indications and warning systems and collection management systems; inputting intelligence data into a variety of ops/intel systems; performing office automation functions; and performing multi-media functions such as voice electronic publishing and video teleconferencing."[3]

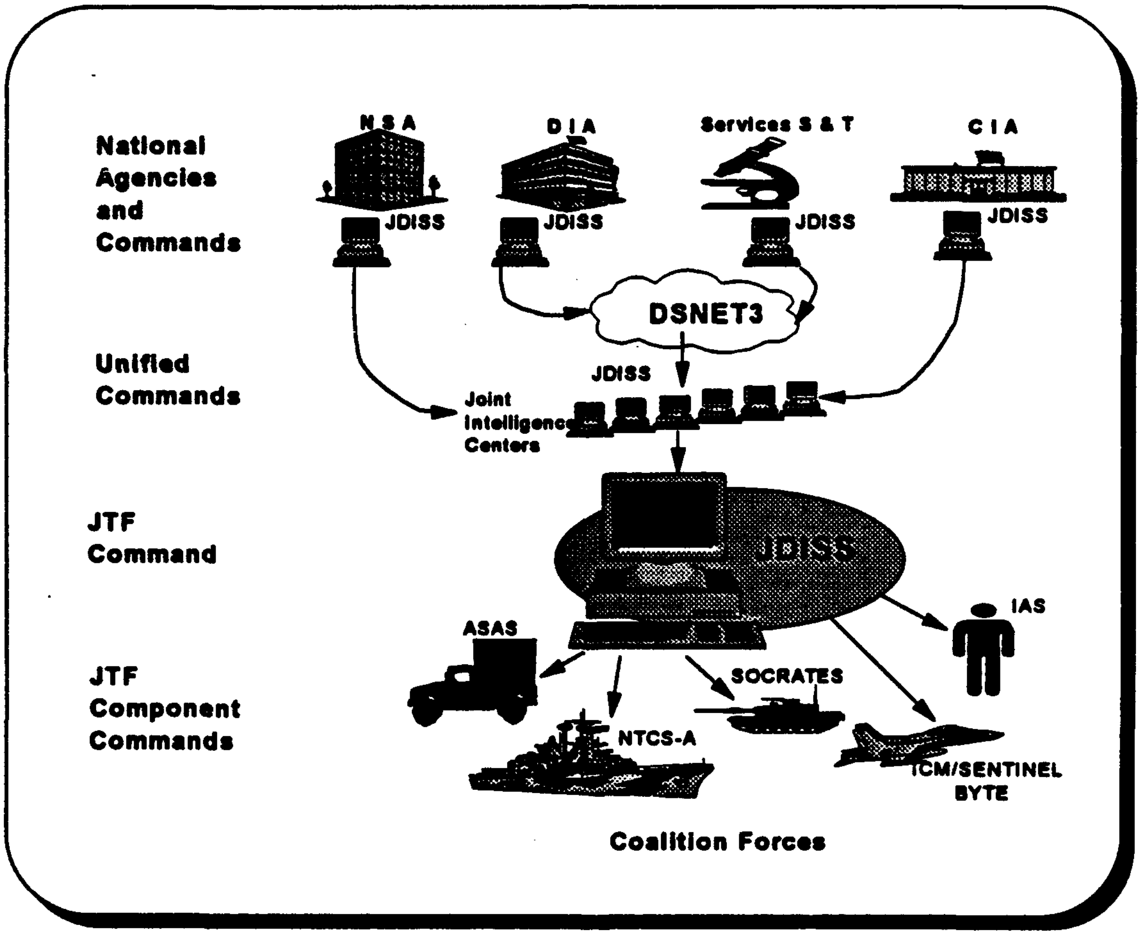


Fig. 5. JDISS Network

Source:JDISS Program Management Office, Joint Defense Intelligence Support Services, (Suitland, MD, 1993): 2.

The connectivity of JDISS currently involves a number of national and tactical systems in varying degrees of operational effectiveness. National interfaces include connections to agencies such as NSA, DIA, CIA, and Service Scientific and Technical staffs. These national agencies are linked through JDISS to the JICs of the Unified Commands. Component command interfaces include the Army's ASAS, the Navy's NTCS-A, the Air Force's ICM/ Sentinel Byte, and the Special Operations Command's SOCRATES.

JDISS recently received interim authority from DIA to be the technical baseline for the DoDIIS client-server environment. This allows JDISS to standardize system services and support to intelligence applications throughout the intelligence community. A key feature is the step toward interoperability in which applications used in any one system will be shared with all systems in the network. Emphasis is placed on the use of readily available commercial off-the-shelf software in order to overcome deficiencies in current hardware and software and to capitalize on the speed and efficiency of commercial systems.

The XVII Airborne Corps and the U.S. Marines have used JDISS on a variety of exercises and the system has proved invaluable in linking tactical users to national databases. The ASAS Program Office is now planning the integration of the JDISS software suite into the Portable ASAS workstation (PAWS).

All Source Analysis System

The All Source Analysis System (ASAS) is being fielded to tactical U.S. Army units. The 82nd Airborne Division fielded the first operational system in September 1993 and XVIII Airborne Corps Headquarters began fielding

ASAS in January 1994. The Army Green Book describes ASAS as "the automated central nervous system guiding field commanders to successfully execute AirLand Operations and is the intelligence-electronic warfare (IEW) subelement of the ATCCS. ASAS automates command and control of IEW operations and intelligence fusion processing."[54] ASAS is the Army intelligence community's contribution to the Army Tactical Command and Control System (ATCCS).

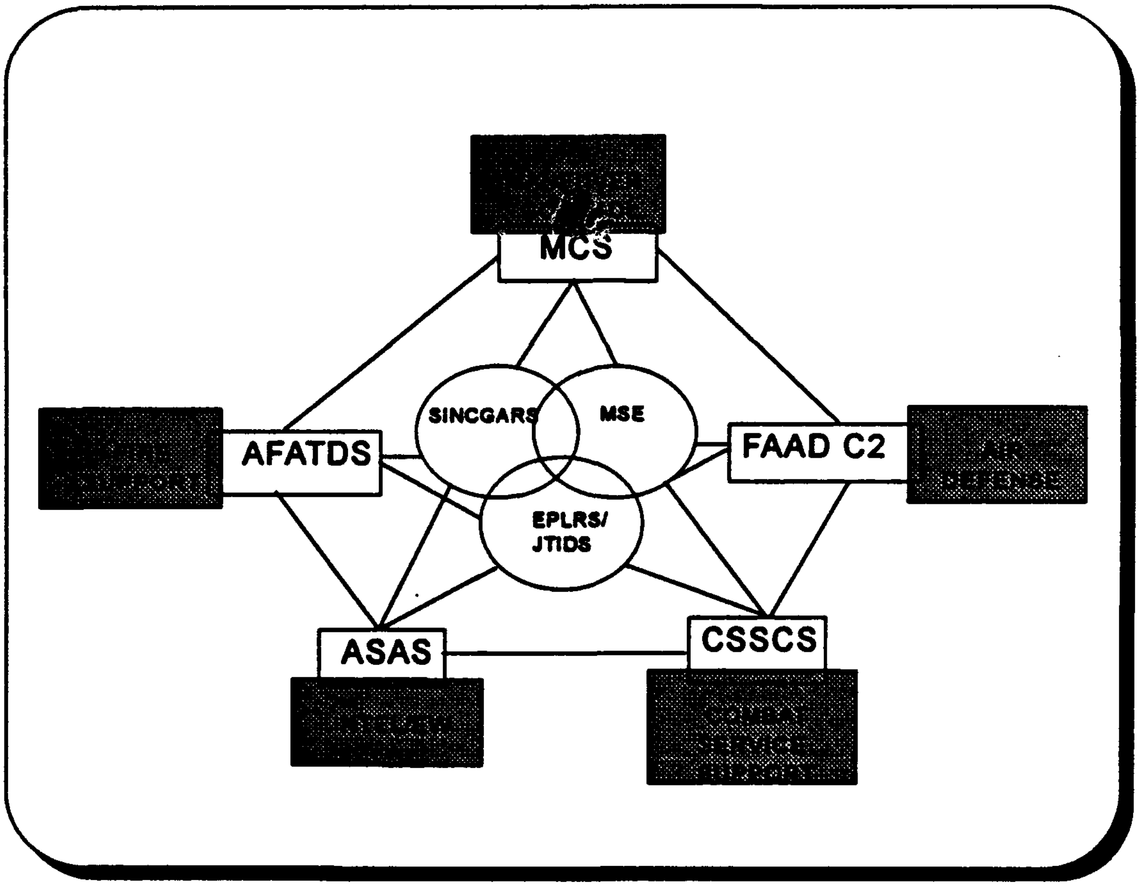


Fig. 6. Integration of ASAS into ACCS.

Source: Program Executive Office, Command and Control Systems, "Army Tactical Command and Control: The Force Multiplier," (Ft Hood,Tx: January 1992).

ASAS, as described by the Army Intelligence Center and School is "a modular, tactically deployable, computer assisted IEW processing, analysis, reporting and technical control system."[5] It provides automated intelligence and information management, and includes an interface to IEW sensors, preprocessors, and the Force Level Control System (FLCS). The interface to the FLCS continuously updates current IEW and enemy situation information to ATCCS and FLCS users. ASAS provides automated support of five primary functions: intelligence development (including indications and warning), target development, collection management and dissemination, electronic warfare support, and counterintelligence and OPSEC support.[6]

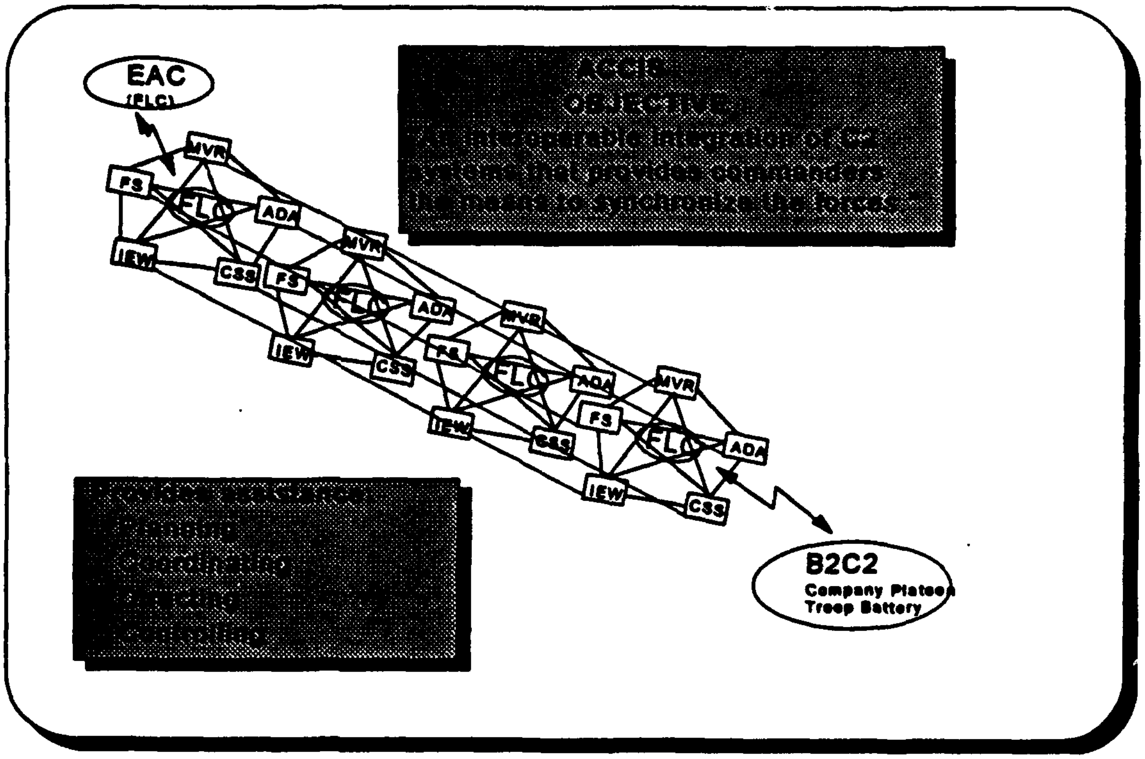


Fig. 7. Army Command and Control System

Source: Program Executive Office, Command and Control Systems, "Army Tactical Command and Control: The Force Multiplier," (Ft Hood,Tx: January 1992).

ASAS includes a host of hardware and software components to support intelligence and electronic warfare. It includes full communications operability to ATCCS as part of the IEW node through Mobile Subscriber Equipment (MSE), TRI-TAC, and other communications systems and area communication subscribers. ASAS receives collateral and SCI intelligence data from a variety of organic unit ground based and airborne sensors, as well as through theater and national intelligence assets. It automatically logs, routes, and stores to the appropriate analyst workstation message traffic information for further manipulation; also it receives and correlates sensor data with multiple reports of like sensor data to produce a machine generated "fused" entity in the database. In addition, software algorithms also correlate intelligence reports from divergent sources and make the resulting correlated database product available to all analysts on the local area network (LAN). Depending on the mission of the unit, the centralized database could include COMINT, ELINT, and All Source information. Analysts can query the database to retrieve relevant data and use the graphics capability to generate a common picture of the battlefield. Included with the ASAS system is the communications and security control system required to allow data to be distributed to other ASAS analysts and to battlefield commanders via ATCCS.

The ASAS system has no resident databases integrated into the system but maintains a database structure which is compatible with the Military Intelligence Integrated Data Systems (MIIDS) Intelligence Database (IDB). Users can download static databases from national agencies or their next higher headquarters via modem and can manipulate the data at the individual workstation. The system uses a relational database management system, which allows common fields from one database to be updated by another database entry, to support the correlation and other functions. It accepts HUMINT reports and makes them available in the form of reference files and as inputs to the fused databas.. The all source capability continually provides updates to intelligence databases to include the national, historical, and friendly order of battle databases. Within the G2 section, situation analysis, target analysis, and collection management, each has access to the fused data and each has specific software functionalities which support its intelligence discipline.

A key element of ASAS is the organizational structure of the G2 section. Of primary significance is the G2 Collateral Enclave. The collateral enclave updates the enemy portion of the Force Level Command and Control System (FLCCS) database, the core of ATCCS, and ensures a single common picture of the enemy for all ATCCS users. Since ASAS will initially operate at the "system high" security level and will process both collateral and Sensitive Compartmented Information, this man-in-the-loop process will be essential until the objective system capably operates with "multi-level security" and conducts data exchange across the Defense Integrated Secure Network (DISN) at both the collateral and Sensitive Compartmented Information (SCI) levels[7].

Of primary importance to this study in the development of ASAS is the identified requirement for connectivity to allied partners. The August 1993 Operational Requirements Document for ASAS states that ASAS "must be capable of interfacing with national, joint (e.g. JDISS), allied (e.g. Battlefield Information Collection and Exploitation System), other service (e.g. Naval Tactical Command System- Afloat, Intelligence Analysis System),"[8] and Army command and intelligence systems and sensors. The requirements document gces on to identify interfacing with future or emerging systems and networks as a major objective. These requirements represent a significant step toward recognizing and integrating allied partners, at least in Europe, but do not adequately address the more difficult problem of interfacing with potential coalition partners. A look at a developing system in Europe will provide insight to potential solutions for other allies and coalition partners.

Linked Operations-Intelligence Centers Europe

The Linked Operations-Intelligence Centers Europe (LOCE) is a U.S. automation information system designed to provide a shared intelligence picture to its customer base. In 1981 the U.S. Office of the Secretary of Defense (OSD) established LOCE and in 1987 the system was officially designated as the U.S. "gateway" to NATO's future Battlefield Information Collection and Exploitation System (BICES). Although originally designed for fewer than twelve remote workstations the network now supports virtually every NATO command center from SHAPE Headquarters to Corps level. Most recently, in 1990-91, LOCE supported USEUCOM and NATO operations during operations Desert Shield and Desert Storm and now supports planning in former Yugoslavia.[59]

The LOCE mission statement calls for the system to provide "near-real-time all-source, correlated air, ground, and naval situation intelligence; finished, validated intelligence products in the form of Order of Battle (OB); and imagery (releasable to NATO) to support situation assessment, threat analysis, targeting, indications and warning, and collection management functions for theater commands."[60] It is fulfilling the mission by crossing service and national boundaries through an open systems architecture which allows interconnectivity of other networks. Most significantly LOCE has made accessable otherwise inaccessible networks such as connectivity to the German Joint Analysis System for Military Intelligence (JASMIN) and the NATO Central Region Command and Control Information System (CR-CCIS). Interfaces include relatively unsophisticated interfaces via floppy disk transfers to U.S. national systems such as IDISS-Europe.

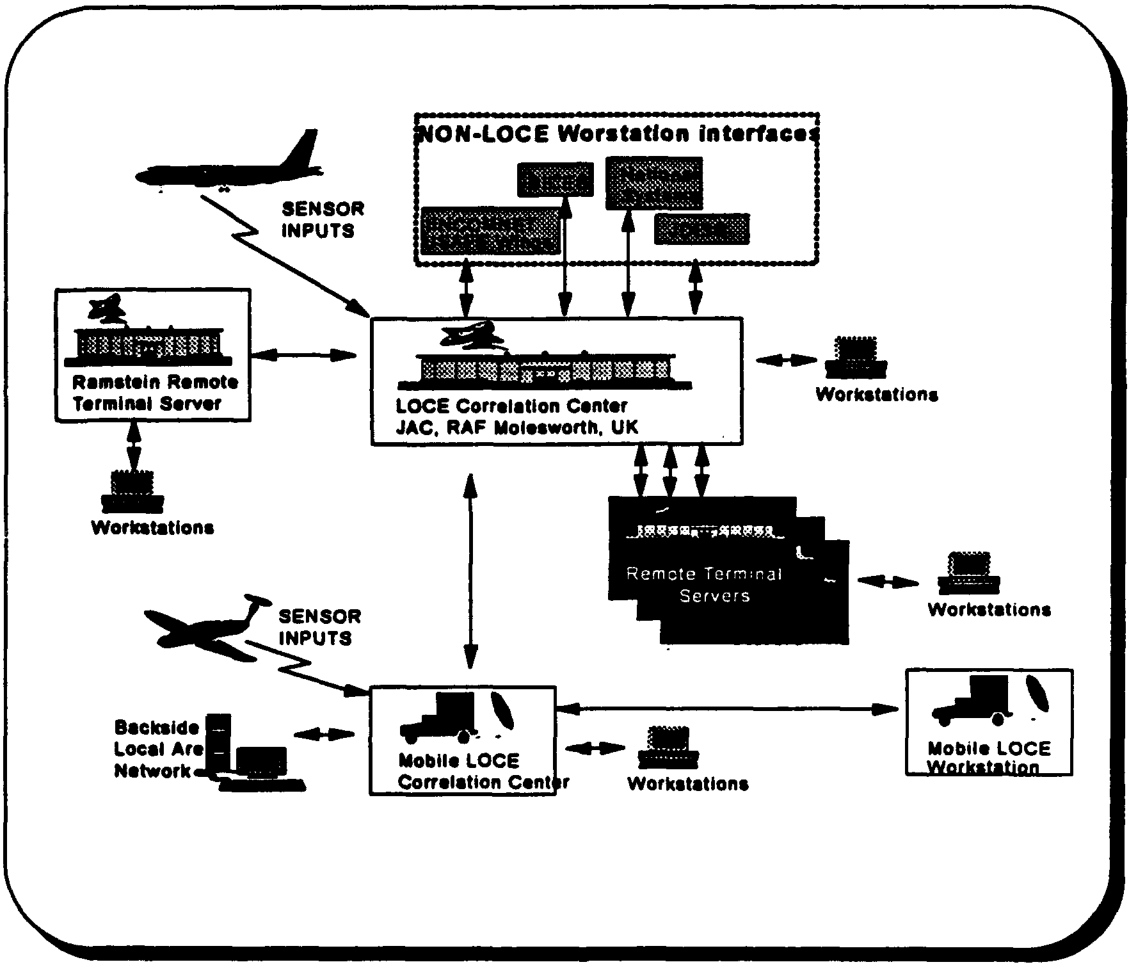

NON-LOCE Worstation interfaces
SENSOR INPUTS
Ramstein Remote Terminal Server
LOCE Correlation Center JAC, RAF Molesworth, UK
Workstations
Workstations
Remote Terminal Servers
Workstations
SENSOR INPUTS
Backside Local Are Network
Mobile LOCE Correlation Centr
Workstations
Mobile LOCE Workstation

Fig. 8. LOCE Network

Source: LOCE PMO, Linked Ops-Intel Centers Europe Workstation, (Arlington, VA, June 1993):1-1.

The LOCE system consists of user terminals linked via encrypted communications to a Correlation Center (CORCEN) located at the new Joint Analysis Center at RAF Molesworth, UK. A program office in Washington, D.C., manages the system under OSD for C3I. The Joint Tactical Fusion Program Office initially designed LOCE as a parallel project of the Army's ASAS and the Air Force's Enemy Situation and Correlation Element (ENSCE) project and deliberately procured it to support the European Central Region in defining requirements for future systems in Europe.

What distinguishes LOCE from other automated intelligence systems is its design to share information with allies. Initially it shared information only with NATO, but with expansion it includes other partners through bi- or multi-lateral arrangements. In fact over seventy LOCE terminals are located throughout the European theater with more planned. Tne data in LOCE is classified at the "U.S. SECRET *releasable to* NATO" level. Consequently, members only need authorization to enter the network and to receive this level of classification.

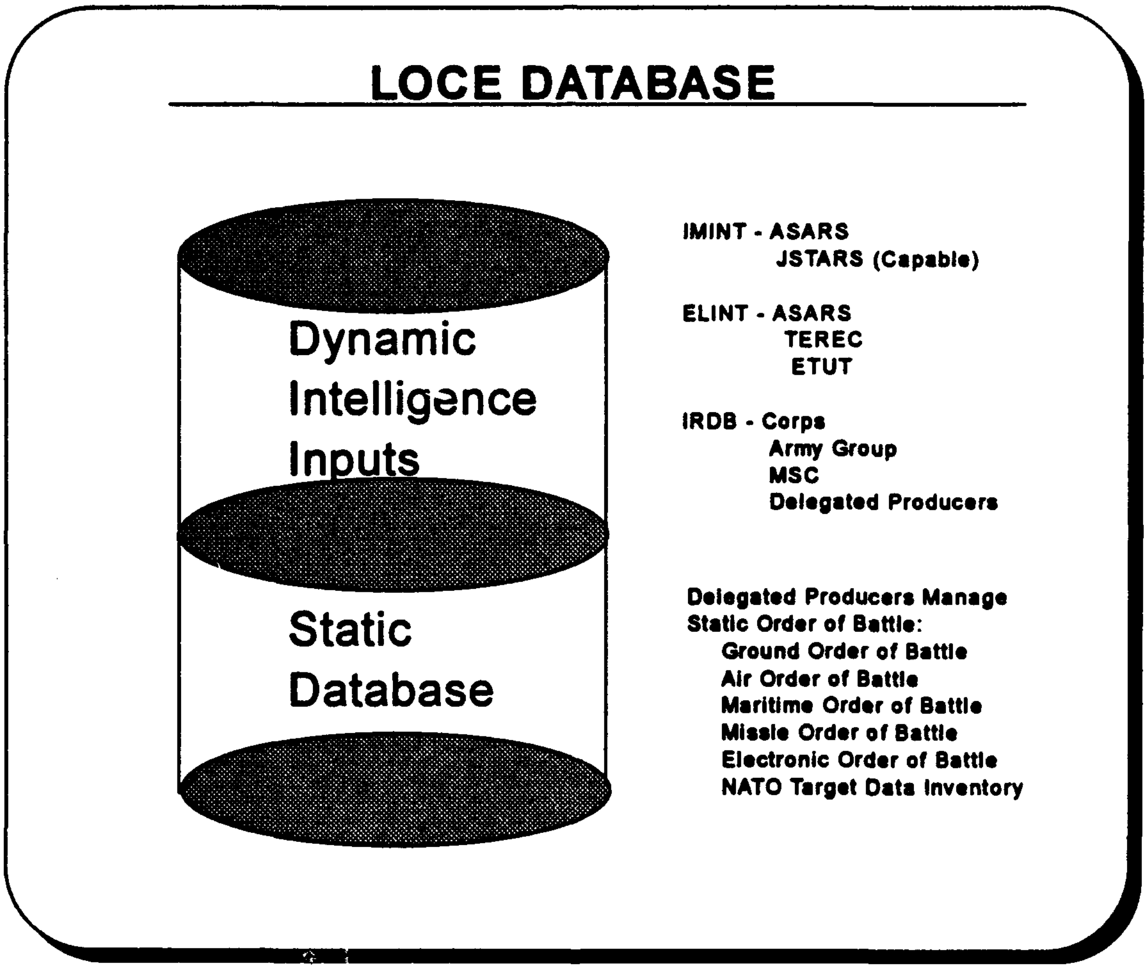
The LOCE architecture is an extended star network with the correlation center (CORCEN) located in the UK. It is considered extended because most of the LOCE workstations are not directly connected to the CORCEN but are connected to local hubs called Remote Terminal Servers (RTS). The RTS has a terminal server, internet router, electronic-mail server, and a digital circuit switch function. The architecture uniquely provides secure voice and data, as well as facsimile, as integral parts of the system. A combination of satellite and of leased terrestrial lines supports the network. A nine meter satellite teleport supports the CORCEN in Molesworth, UK, and a 2.4 meter towed remote satellite dish supports a mobile correlation center concept. With

NATO provided satellite communications, the network extends to a footprint encompassing the entire EUCOM area of interest, from Norway to Turkey, and back to the United States.

The strength of LOCE is the database which provides correlated data on real and potential threats in all operational dimensions. The database is populated and maintained through a distributed database management approach in which delegated order of battle managers are responsible for particular databases. These order of battle managers are intelligence producers with expertise in the various collection disciplines or in the specific geographic area of interest defined for their wartime headquarters. Increasingly, these sources are non-U.S. information managers. The database consists of static data, maintained by delegated intelligence producers, and dynamic data primarily input through sensor interface modules by ELINT and IMINT sensors. The following identifies the delegated intelligence producers and the order of battle managers for the static data bases:

Ground Order of Battle -	Army Corps (international)
Air Order of Battle -	Allied Air Forces, Central Europe
Naval Order of Battle -	Allied Forces Northern Europe
Electronic Order of Battle-	USEUCOM, Joint Intelligence Center
Missile Order of Battle -	Allied Air Forces, Central Europe
NATO Target Data Inventory -	USEUCOM
Collection Coordination Intelligence Requirement Management	- USEUCOM

The overall database management, in a political environment such as NATO, significantly concerns all members of the network. Consequently, the users with input privileges must have a recognized expertise and a verifiable collection capability. An agreed upon hierarchy of privileges and restrictions allows certain users to add to or delete from the database; therefore the delegated producers maintain control of their particular responsibilities, but all members of the network maintain the capability to read from the database.



LOCE DATABASE

IMINT - ASARS
JSTARS (Capable)

ELINT - ASARS
TEREC
ETUT

IRDB - Corps
Army Group
MSC
Delegated Producers

Delegated Producers Manage
Static Order of Battle:
Ground Order of Battle
Air Order of Battle
Maritime Order of Battle
Missle Order of Battle
Electronic Order of Battle
NATO Target Data Inventory

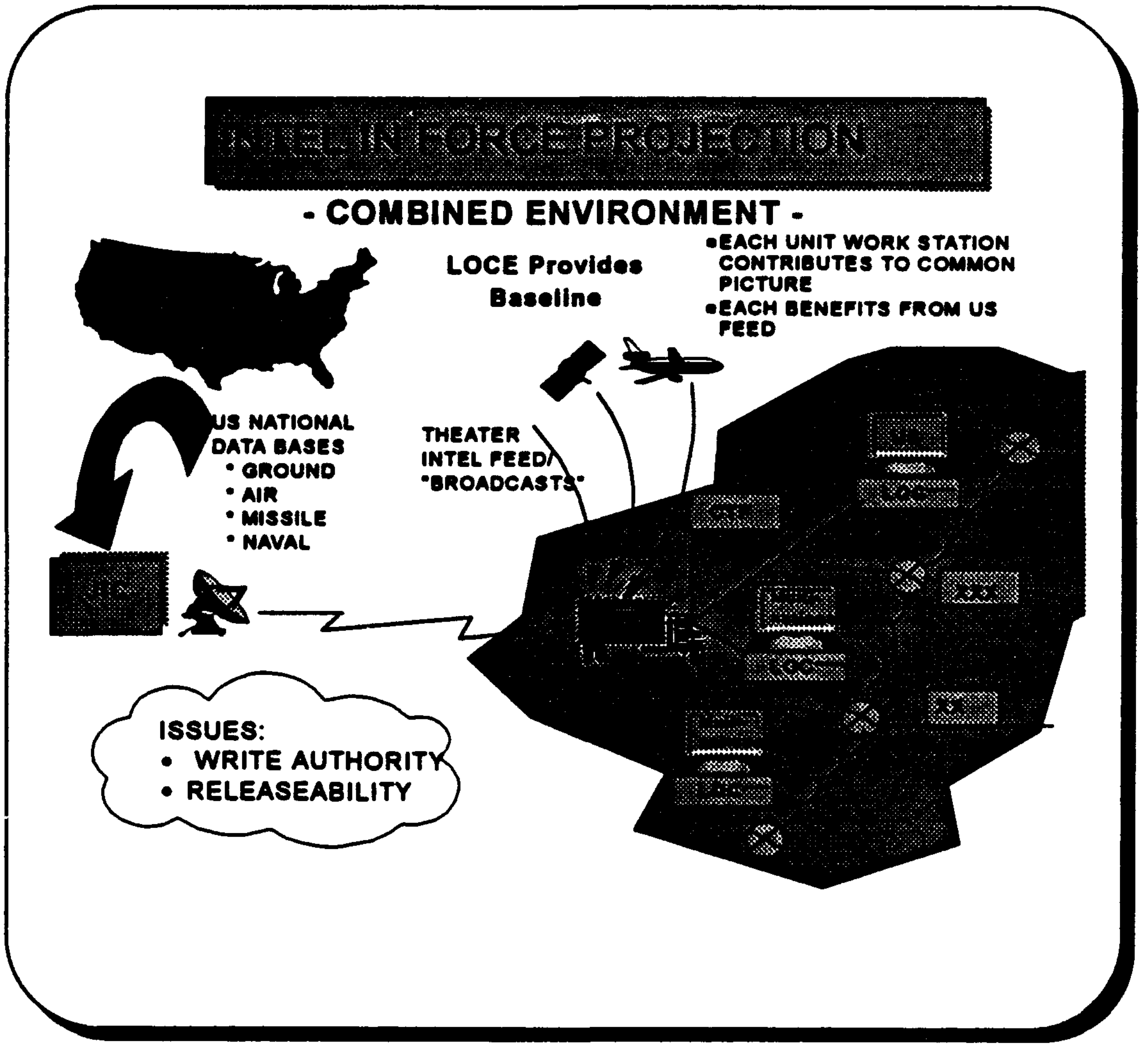
Fig . 9. LOCE Database

Of almost revolutionary importance to the intelligence community are the dynamic feeds and inputs from other nations. In addition to the manual inputs from the various intelligence producers, LOCE connects with several collection systems which provide near- real-time data in the form of ELINT and IMINT. This dynamic portion of the database is called the Individual Reports Database (IRDB). The source of this information comes from a variety of NATO, U.S., and allied sensors. NATO's control of the TR-1 (U-2) is of vital importance to the entire collection process and releasability issue. The fact that NATO controls a collection system with imagery and electronic intelligence capabilities paves the way for national agencies to input like sources of information under the guise of "plausible cover." Members of the network can access all of this information by simple queries, and the results can display in the form of a text format and digital mapoverlays.

The future of LOCE will lie with its ability to change with evolving world politics. As contingencies arise, commanders and intelligence staffs will require a computer information system like LOCE to provide a common picture of the area of interest. The EUCOM staff contends that there is a place for LOCE to support arms control treaty monitoring and verification activities, counter-terrorism efforts, and counter-narcotics initiatives generated by EUCOM. The use of new technologies like the multi-media digital studio (currently installed) will allow EUCOM to conduct intelligence briefs similar to Cable News Network (CNN) and to revitalize analytical exchange of ideas and information. Future automated direct down links from sensors, as well as an enhanced imagery transfer capability, will make LOCE a viable system for coalition and peacekeeping operations within NATO.

The LOCE system currently meets the original goals set by the founders in 1981 and has potential for laying the foundation for future gateways to all allies and coalition partners. The project managers working C4I for the Warrior are interested in using LOCE as part of their quickfix link to NATO.

MG Stewart, currently the Commanding General of the U.S. Army Intelligence Center, during his visit to the CGSC, described how he envisions a "LOCE-type" system that can be applied not only to NATO, but also to any conflict in the world.



INTEL IN FORCE PROJECTION

- COMBINED ENVIRONMENT -

LOCE Provides Baseline

- EACH UNIT WORK STATION CONTRIBUTES TO COMMON PICTURE
- EACH BENEFITS FROM US FEED

US NATIONAL DATA BASES
- GROUND
- AIR
- MISSILE
- NAVAL

THEATER INTEL FEED/ "BROADCASTS"

ISSUES:
- WRITE AUTHORITY
- RELEASEABILITY

Fig. 10. LOCE as an interface in combined operations

Source: John F. Stewart, "MI Corps Intelligence Strategy - Intelligence in Force Projection," Briefing to CGSC Intelligence Officers, Ft Leavenworth, K3, 4 August 1993.

C4I for the Warrior: A Concept for the Future

From the womb of the National Military Strategy emerged the C4I for the Warrior concept, briefed to the Secretary of Defense, the Chairman of the Joint Chiefs of Staff, and the Joint Chiefs of Staff in February 1992. This concept envisions a fused, real-time presentation of the Warrior's battlespace. "The capability of the Warrior to respond and coordinate horizontally and vertically to prosecute effectively and successfully any mission in the Battlespace is the essence of the C4I for the Warrior concept."[61] It recognizes that the current C4I systems do not have sufficient interoperability, especially from a functional integration perspective.

The Chairman of the Joint Chiefs of Staff is fully committed to making the C4I for the Warrior concept a reality. He believes that the concept must be fully institutionalized this year not fifteen years from now. In a speech to the House Appropriations Committee on 5 March 1993, General Powell said, "We still have a long way to go, but we have now developed the momentum and unity of effort to keep us moving forward toward achieving the C4I for the Warrior objective." [62] General Powell based his remarks on a road map detailed by his staff over the past year. When first conceived, a comprehensive, acheiveable roadmap for reaching the objective was essential to maintaining the momentum of the project.

The three phases of the C4I for the Warrior concept intially announced in 1992 were: (1) Quickfix Phase, (2) Mid-Term Phase, and (3) Objective Phase. Lieutenant General Albert Edmonds, Director of the Command, Control, Communications, and Computer Systems , J-6, of the Joint Staff acknowledges that we have achieved the Quickfix phase. The Quickfix Phase is the near-term improvement toward interoperability. The fixes include the integration of translators that receive dissimilar message formats and communication protocols and the exchange of data through standard transmission routines. Since noi all of the message formats and communication protocols are standard, technical Tiger Teams are identifying the systems which must be interoperable and will best contribute to the mid-term and objective phase goals. All other systems shall be obsolete over the constructive lifetime of the software and hardware.[63] During the mid to late 90's we will enter the Mid-term Phase which will result from the technological break-throughs developed in the Quickfix Phase. The Mid-term Phase will produce a comprehensive web of networks all working together within a joint framework. This stage will mark the beginning of the fulfillment of the void of "fused" information required by tactical decision makers. [64] As we enter the 21st Century, we shall move into the Objective Phase. The primary objectives are the development of "a multifunctional, multimedia terminal fitted to meet all of the Warrior's functional requirements; a battlespace that provides totally fused information and a fully integrated tactical picture; and an infosphere which is global in nature."[65]

In order for the C4I for the Warrior concept to evolve naturally, the JCS recognizes that it must be fully integrated into a solid foundation and has taken steps to ensure that this concept is fully integrated into the current strategy, policy, and doctrine. Annex C of the National Military Strategy Document identifies C4I system interoperability as the number one C4I program objective. The revision of policy documents underscores the new policy of C4I interoperability, and the principles and tenets of the C4I for the Warrior concept are now being documented in joint, as well as, service publications.

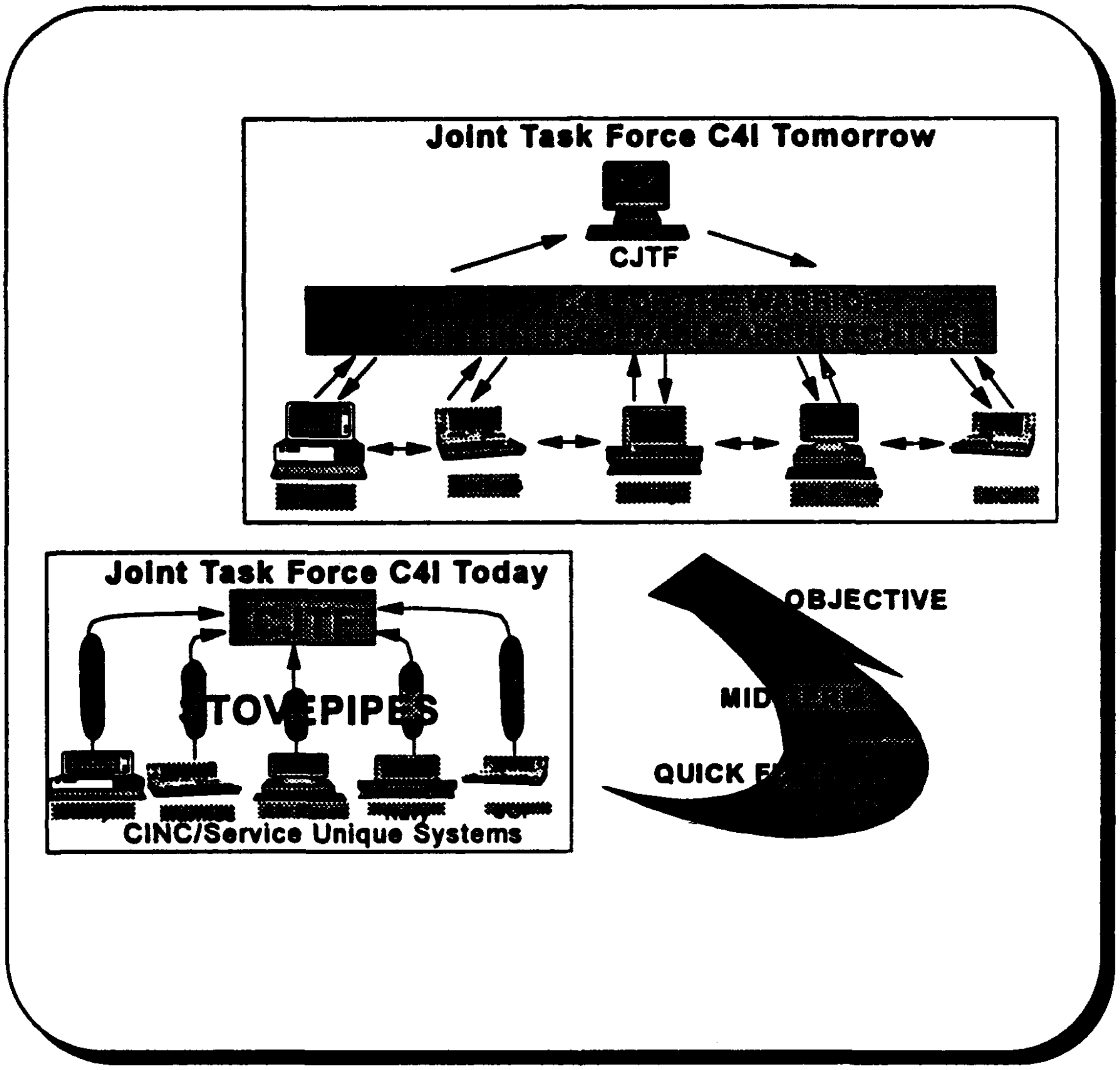

Joint Task Force C4I Tomorrow
CJTF
Joint Task Force C4I Today
CJTF
STOVEPIPES
CINC/Service Unique Systems
OBJECTIVE
MID
QUICK F

Fig. 11. C4I for the Warrior Concept

Source:The Joint Staff, C4I for the Warrior, (Washington, D.C.:U.S. GPO, June 1993): 2.

The Joint Staff laudes the C4I for the Warrior concept as a "new way of doing business." It will inherently affect four major areas within the C4I community: organizations, standards, testing, and acquisition. Organizationally, we shall find a more streamlined and integrated process to identify and resolve interoperability issues in a more effective and responsive manner.[66] The Joint Staff is reviewing the C4I standards to identify current interoperable architectures and the Defense Information Systems Agency (DISA) has established a focal point for standards development. The new Center for Standards will place emphasis on examining commercial standards to meet military requirements. Testing will emphasize an operational scenario to ensure all new systems comply with all interoperability requirements. Acquisition procedures will change from the single service approach to a common approach.[67]

The C4I for the Warrior depends heavily on many ongoing efforts. Joint exercises are vital not only to refining doctrine and procedures but also to testing the success of new software and battlefield electronics.[68] Combined interoperability issues with NATO and Pacific allies focus extensively toward the release and development of standards and standard agreements. Within the U.S. military community, much has been accomplished since August 1992 with the achievement of database interoperability and with the comparison of the U.S. Message Text Formats (USMTF). Of significance is the MIIDS IDB structure developed by DIA. [69]

In addition to the ongoing efforts, the Joint Staff is pursuing a number of proofs of concept. Based on the results of a C4I for the Warrior Tiger Team, the Naval Electronics Systems Engineering Activity (NESEA) concluded that a quickfix to the technical interoperability problems could be resolved with a "translator" based on a set of thirteen data formats. Also NESEA has developed the Joint Universal Data Interpreter (JUDI) which will allow interoperability between a number of major C2 systems. This new approach provided a framework for the standardization and establishment of a Common Interoperability Language.

Although the description of the intelligence systems chosen for this study is not all inclusive, the highlighted elements of each make them viable systems for the future. Harnessing the information explosion and winning the information war are goals imbedded in each system. Within each of the systems we also find some hint of a requirement to link with allied and coalition forces. We have identified at least one answer for one theater of operation by examining the contributions of LOCE to the eventual development of an objective intelligence architecture for NATO.

Endnotes

[1]JDISS Program Management Office, Joint Defense Intelligence Support Services, (Suitland, MD, 1993), 2.

[2]Ibid., 2.

[3]Ibid., 2.

[4]Army Weaponry and Equipment," Army Green Book 42 (October 1992), 284.

[5]Intelligence and Electronic Warfare (IEW) System Fact Sheets," (Ft Huachuca, AZ, 1993), 45.

[6]Department of the Army Memorandum, "Operational Requirements Document (ORD) for the All Source Analysis System," (Washington, D.C., August 1993), 5.

[7]Ibid., 2.

[8]Ibid., 15.

[9]USEUCOM, Joint Analysis Center, LOCE Division, Linked Operations Intelligence Centers Europe, (RAF Molesworth, UK, 1993),1.

[10]LOCE PMO, Linked Ops-Intel Centers Europe Workstation, (Arlington, VA, June 1993), 1-1.

[11]The Joint Staff, C4I for the Warrior, (Washington, D.C.: U.S. GPO, June 1993), 2.

[12]Ibid., 15.

[13]Ibid., 16.

[14]Ibid.

[15]Ibid.

[16]Ibid., 19.

[17]Ibid., 20.

[18]Ibid., 21.

[19]Ibid., 22.

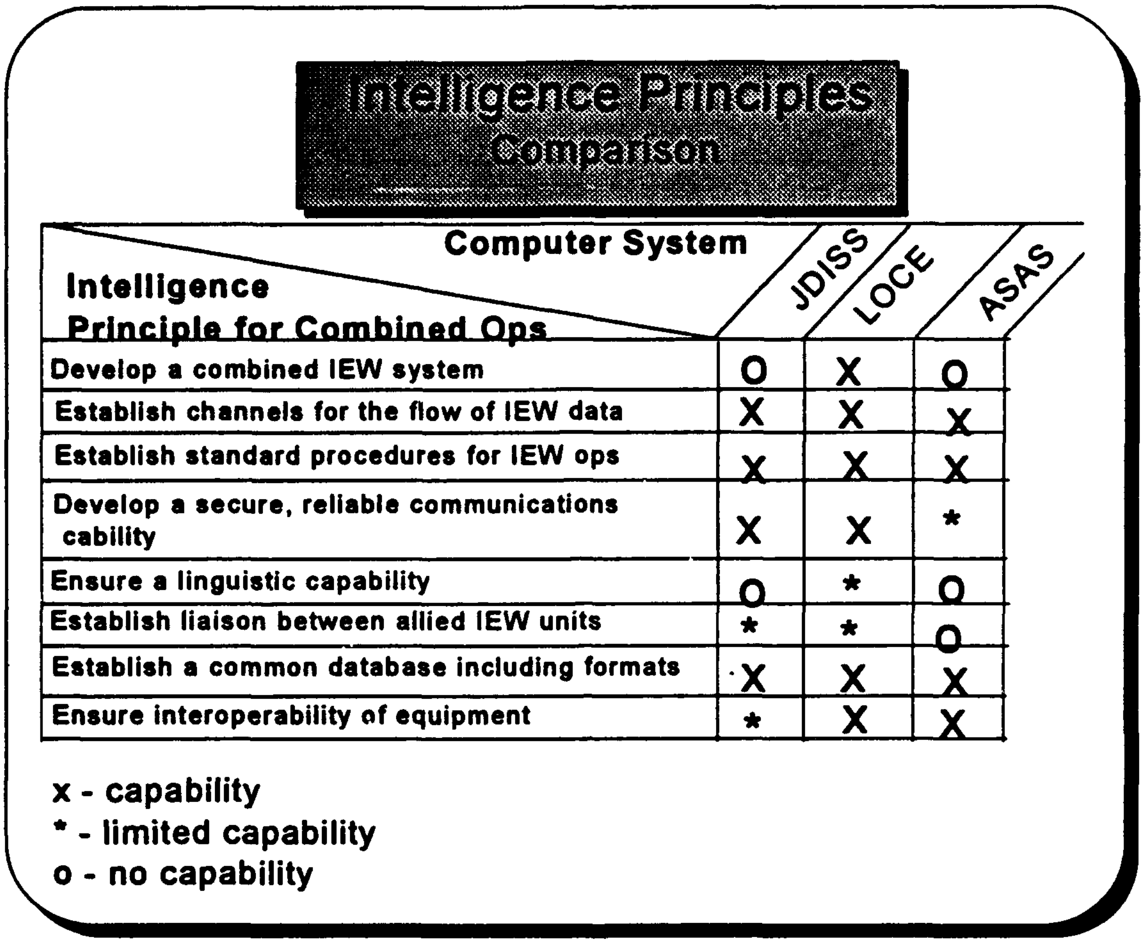
CHAPTER 6

ANALYSIS AND CONCLUSION

Initially, the problem statement as defined by this thesis was the identification of the requirements of a multinational intelligence system for the force projection Army of the future. The historical and descriptive portion of the methodology are the basis for the comparative analysis. In this study we have briefly reviewed the current doctrine as it applies to joint, combined and Army operations, to the intelligence lessons learned in the most recent conflicts, and to some of the most significant intelligence information systems at the tactical and operational levels of war. Additionally, we have taken an in-depth look at the C4I for the Warrior concept of the future and concluded that the developing systems have met the quickfix phase and will be the backbone for the objective architecture. Finally, using the results of the study as a foundation, we shall analyze the current systems based on the principles of intelligence for combined operations and proceed to evaluate the C4I for the Warrior concept as it applies to intelligence using the CGSC SAM.

Analysis

The analysis is based on how well the current systems meet the principles of intelligence in combined intelligence operations. The following chart depicts the intelligence principles for combined operations and compares the three systems chosen for this study.



Intelligence Principles Comparison

Intelligence Principle for Combined Ops \ Computer System	JDISS	LOCE	ASAS
Develop a combined IEW system	O	X	O
Establish channels for the flow of IEW data	X	X	X
Establish standard procedures for IEW ops	X	X	X
Develop a secure, reliable communications cability	X	X	*
Ensure a linguistic capability	O	*	O
Establish liaison between allied IEW units	*	*	O
Establish a common database including formats	X	X	X
Ensure interoperability of equipment	*	X	X

x - capability
* - limited capability
o - no capability

Fig. 12. Comparison of Intelligence Principles for Combined Operations. JDISS Analysis

The systems were assessed based on their capability to adhere to the principles, to provide a limited capability, or to provide no capability. When judging limited or no capability, the review of system requirements documents to assess the developers plan for the future played an important part of the overall assessment. For example, the ASAS requirements document identifies a future need to interface specifically with a LOCE or BICES capability within NATO. Since LOCE and ASAS have similar software, derived from the same core set of applications software, and since the communications protocols will be coordinated within NATO, a rating of limited capability applies. Conversely, JDISS already has a limited interface with LOCE via a man-in-the-loop floppy disk transfer and generates a rating which reflects the system as having a capability to meet the intelligence principle being measured. Since the ratings are a subjective judgment, each of the systems and their ratings will be discussed as they apply to the chart and to the principles of intelligence for combined operations.

This study first concentrated on JDISS, which is essentially a client server network that maintains a core set of applications which conform to DoD standards. In the most simplistic terms this system is not truly an intelligence fusion system, but a gateway for tactical and operational level intelligence fusion systems to pull intelligence data from national sources and to exchange data within the network. There is no intelligence "fusion" accomplished in the JDISS system, but intelligence personnel need access to these applications and databases to conduct fusion as we understand fusion today. However, access to the network does not automatically imply authorized access to all the databases available in the JDISS network. Users apply for access on a "need to know" type basis to each of the national databases accessable through JDISS. Since JDISS is a U.S. only system, it can not be rated as part of the combined IEW system; nevertheless many of the databases available may, in fact, be the basis for a combined commands initial static database. For example, the NATO Target Data Inventory (NTDI), which catalogs all targets within NATO, is essentially a subset of DIA's Automated Installation File (AIF).

The JDISS program managers are working toward interoperability with combined intelligence operations. JDISS and LOCE have already begun work toward establishing a flow of intelligence data from JDISS to LOCE through JDISS-Europe (JDISS-E). This current interface requires an air gap, in which a man-in-the-loop conducts a floppy disk transfer, since no current technology meets the standards of security and multi-level security as required by DIA to connect physically to a Secret Releasable to NATO system. However, the interface requirements identified to conduct a floppy disk transfer or tape-to-tape transfer provide the basis for identifying and establishing future standards between U.S. and NATO systems. Although JDISS does maintain a core set of standards, purely the adherance to standards does not guarantee interoperability. Standards established by DoD and the civilian community are implemented and continue to evolve, but today many are not robust enough to ensure complete interoperability as the creators did not envision future capabilities and did not build open architectures. In some cases, standards are non-existent.

Central to all intelligence systems are the communications which support the transfer of data. The communications backbone of the JDISS system allows connectivity to virtually any combined operation. As JDISS and LOCE both have the luxury of maintaining fixed sites for the hub of their networks, they both take advantage of high throughput with a wide variety of military and civilian communications systems. As each of the unified commands has selected JDISS for implementation in their Joint Intelligence Centers (JICs), communication to deployed Joint Task Forces, also equipped with JDISS, can be facilitated. Additionally, from a strategic to operational level, the support of JDISS emanates from the Pentagon through the use of

National Intelligence Support Teams (NIST) composed essentially of DIA, CIA and NSA liaison officers and a JDISS terminal supported by SATCOM. The NIST program is run by DIA and is designed to put a deployable strategic intelligence entry point at the operational level. These liaison teams provide SCI capability only to U. S. headquarters, but during the Gulf War they furnished liaison to both Britain and Turkey. Although JDISS can provide a limited capability within security restraints in the form of liaison between allied IEW units, a robust combined intelligence network is not currently envisioned.

The three major deficiencies noted of JDISS in support of combined operations are the linguistic capability, multilevel security, and the interoperability of equipment with allies or coalition partners. As far as the research can determine, JDISS has no apparent ongoing or future initiative, nor any charter to integrate multiple languages into the system. Since it does not maintain a database but merely allows an interface, this sytem could be part of the multi-level security solution but it will not solve the problem. The equipment interoperability issue would be an easy fix if the JDISS program could give JDISS terminals to every nation envisioned as a potential coalition partner; although this, too, would be an economically infeasible solution. As a client server network, the JDISS program focuses on the lower interoperability levels, and it leaves much of the higher level interoperability issues up to other programs such as ASAS, LOCE, and the international community building systems such as BICES in Europe. The following figure depicts the interaction of the systems with the levels of interoperability. The interoperability issue emerges in degrees or stages and becomes increasingly more complex at higher levels. It ranges from basic cable connections to the most complex issues of a common picture of the battlefield and multi-level security. JDISS, an extremely fast moving project, depends heavily upon the use of commercial software and off-the-shelf commercial equipment. As the issues of interoperability increase in complexity, the other projects may move much slower, but contribute to and build upon the base of the product development of systems such as JDISS. The levels of interoperability also increase as the requirements for the exchange of data and functionality increase.

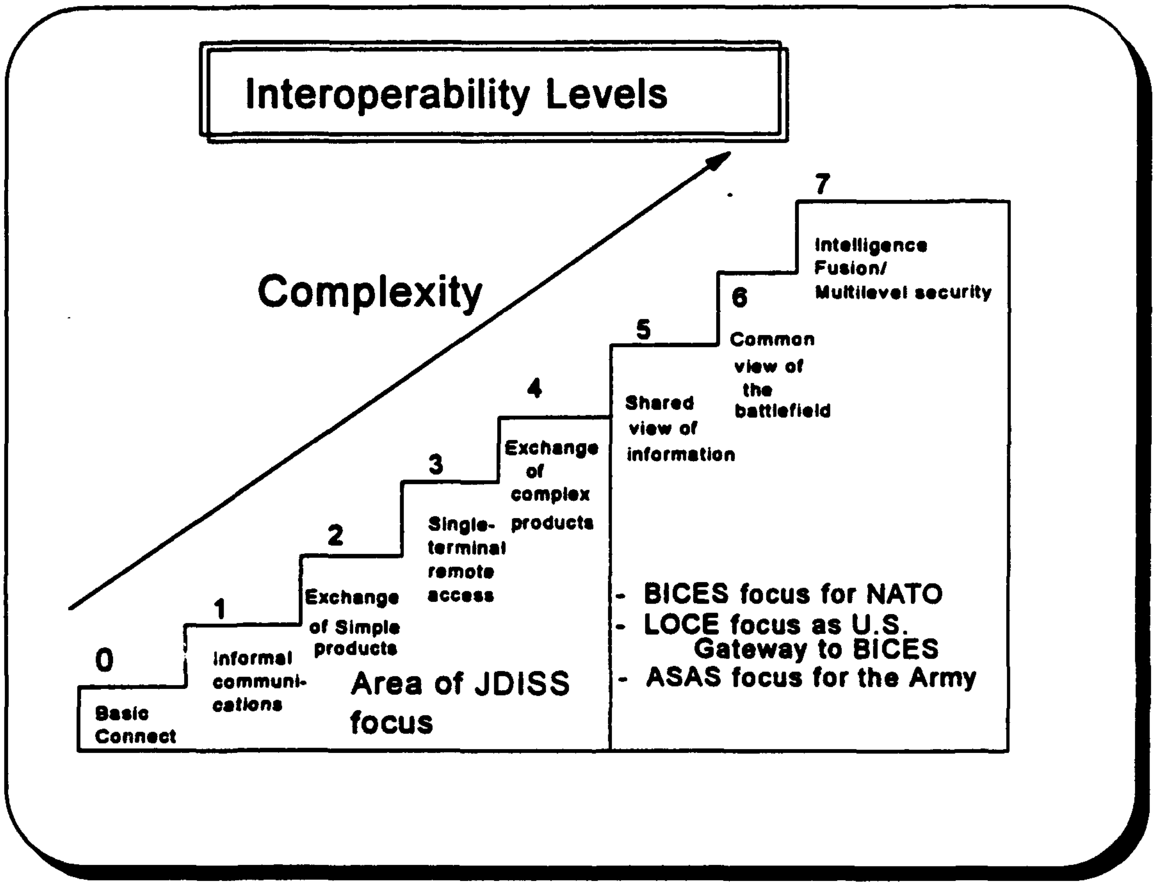

Interoperability Levels
Complexity
0
Basic Connect
1
Informal communi-cations
2
Exchange of Simple products
3
Single-terminal remote access
4
Exchange of complex products
5
Shared view of information
6
Common view of the battlefield
7
Intelligence Fusion/ Multilevel security
Area of JDISS focus
- BICES focus for NATO
- LOCE focus as U.S. Gateway to BICES
- ASAS focus for the Army

Fig. 13. Interoperability Levels

Source: COL Bob Maynard, "An Integrated Set of Common Software Applications," JDISS Program Management Office briefing, Suitland, Md, 1993.

Essentially, JDISS focuses on the first five levels while LOCE and ASAS tackle the more complex issues of database fusion and gateways to allied nations. However, the baseline contributions of the first five levels provide the foundation for accomplishing the higher levels and the final objectives of C4I for the Warrior.

ASAS Analysis

ASAS, like JDISS, has no charter to operate in a combined environment as part of the backbone of a combined IEW architecture. Currently, the concerns over computer information security prohibit the use of ASAS for combined operations. Through the collateral enclave, designed to operate at a secret level, ASAS could potentially sanitize information and, in a manner similar to JDISS, pass information to a combined system. Presently, no procedures are identified for establishing a flow of data to combined headquarters, but since systems such as LOCE and ASAS have the same basic software and the Portable ASAS Workstation (PAWS) can run LOCE software, a limited capability is assessed. Additionally, ASAS has only been officially fielded for less than six months. As the tactical intelligence community becomes familiar with the capabilities of ASAS, new procedures will be developed to exchange data with coalition partners. In fact, ASAS does have a charter to establish a future link with systems such as LOCE and BICES.

Both ASAS and LOCE use the MIIDS IDB database structure created by DIA as a foundation for the structure of service wide intelligence databases. Since LOCE is the U.S. gateway to BICES, ASAS does not need to work combined database interoperability issues, but instead does need to maintain an ușen architecture and does need to influence the development of systems designed for combined interfaces by demonstrating intelligence fusion capabilities. ASAS has gone to great length to build communication processors which interface with a variety of different communication formats and protocols. Much of the power of ASAS lies in its ability to interface with tactical and strategic intelligence systems and systematically to share data within the intelligence staff organization through a local area network.

The major shortfalls of ASAS for use in a combined intelligence system are its lack of language support, its lack of a light weight portable system for liaison officer use, and its limited capability for secure communications between tactical allied headquarters via a multi-level secure means. Since ASAS was designed as a U.S. only system, the language and the interoperability issue will not be solved within the ASAS program. The requirement document for ASAS identifies a requirement to interface through other U.S. systems in the outyears to allied nations. Some ASAS applications software can already provide a limited capability to interface with allied nations. However, the research indicates that no plans exist to establish automated tools for liaison and none will probably be formulated until a multi-level security system is brought on-line. As one travels up the ladder in the levels of complexity for interfacing, only a few systems will tackle the complex issues of total interoperability with allied nations.

LOCE Analysis

The system with the most experience in dealing with combined intelligence operations is the LOCE system. This system meets all of the requirements of combined intelligence operations by providing a full capability in most of the intelligence principles and a limited capability in the remaining intelligence principles. As the U.S. gateway to BICES, LOCE has held the charter to explore interfaces, to assist in development of standards, and to provide a demonstration system for intelligence fusion to NATO. Over the past twelve years, LOCE has provided a testing ground for international database management, for intelligence fusion, for international development of a military data element dictionary, and for muti-language military translation tables. The existence of a LOCE type system has initiated national level discussion on potential solutions to multi-level security and on the value of computer enhanced "mixing" of data in the fusion process to provide plausible cover for the passing of intelligence information to coalition partners. By "mixing" U.S. only with British, German, or French only intelligence information in one large melting pot, the source of the data becomes fused as part of an all source database. The resulting true nature of the report could be attributed to a myriad of sources. The benefit is more intelligence to those countries with less capability and better intelligence to those countries which have greater capability. MG Stewart has identified LOCE as the baseline for a model to provide an intelligence fusion capability in combined operations. Only the major questions of write authority to the database and of national releasability remain. As NATO further refines the requirements for BICES, these issues can be negotiated. The real strength of the system is the current connectivity and the expanding network. It is evident that LOCE will be the basis of the C4I for the Warrior connectivity to NATO and the model for CENTCOM and PACOM to emulate.

Consolidated Analysis

None of the studied systems individually meets all of the requirements identified for intelligence in a combined operation. When taken as a whole, using a combined approach, a comprehensive system in its own right begins to emerge. Further evaluation shows that each system is capable of meeting the elements of intelligence quality within the limits of current technology. Each system serves its own core set of users within a relatively closed environment for security purposes and each provides timely, accurate, objective, and relevant intelligence information. The main deficiency identified, covering the entire spectrum of systems, is **the lack of multi-level security**. Realistically, a total unconstrained exchange of information will never occur among our coalition partners unless security of their information can be guaranteed. The lessons learned of World War II with the allied use of Ultra and Magic vividly exemplify the underestimating the technical *sophistication of the enemy*. Hitler and his staff were convinced that the Enigma machine was totally secure, yet the successes and failures of the Wehrmacht can be directly related to the level of operational security applied. Our current leaders are not naive enough to believe that any system is totally secure. They envision multi-level security capabilities, but currently the technology does not exist which adequately separates Top Secret from Secret and U.S. Secret from Secret Releasable to NATO, etc.. Until then, closed networks and a man-in-the-loop type of approach to intelligence sanitization will continue to exist.

The bottom line for the comparative analysis is that the basis of the principles for intelligence in combined operations is covered when the effects of the three systems studied are brought together. From the strategic database to the tactical sensor, a usable common picture of the battlefield can be achieved in a mature theater. The battlefield commanders require a combined system with the capabilities of all these systems to appropriately achieve the requirements of intelligence fusion for combined operations. C4I for the Warrior embraces a concept to meet these challenges.

C4I for the Warrior: The FAS test

C4I for the Warrior is a concept the military will take into the 21st century to achieve a military information superhighway. The intelligence portion of the overall system will be the U.S.'s answer to intelligence fusion in combined operations. Having reached the quickfix phase, we are now working towards goals established for the mid-term phase. The doctrine is now being written to support C4I for the Warrior, the standards are under development, and the basic building blocks are being fielded. As we consider the three systems just analyzed, we witness the formation of the C4I for the Warrior vision. The feasibility, acceptability, and suitability questions remain.

Feasibility

Feasibility addresses capabilities. Is a certain course of action possible in terms of assets and technology available? What-are the training and skills of the operators? Can the objective be supported logistically, etc.? Although the question in context of Army support to intelligence fusion in combined operations is academic at this point, the answer is affirmative.

The evidence shows that we now have the technology to conduct intelligence information sharing within some security driven guidelines with many of our allies. The crux of the matter is that by merely having a network in place facilitates the inevitable sharing of data. In a crisis situation many of the traditional security doors come down and a much freer flow of information takes effect. If a robust system were initially in place, information previously unavailable may become so simply due to ease of input and ease of access.

While current capabilities vary within the DoD and certainly among our allies, the use of commercial-off-the-shelf (COTS) equipment, an approach endorsed by C4I for the Warrior, certainly enhances the probability that compatibility is possible without an inappropriate amount of U.S. financial assistance. Additionally, the early coordination of interoperability standards among nations, as accomplished in NATO, is encouraging. The standardization of a military data element dictionary and Standard NATO Agreements governing standards and procedures for tactical data links prove that the concept is workable in a combined environment.

Suitability

Suitability focuses on whether or not a particular course of action will produce the desired results. In this case our question focuses on whether the C4I for the Warrior concept can support intelligence fusion in combined operations.

The impact of technology on the modern battlefield and on the command and control process is depicted in the figure below. This chart shows that at the beginning of a military operation, the commander, staff, and all of the subordinate commanders have a better than adequate understanding of the military situation and plan. As time and tempo of the battle increase, the knowledge level of the commander and the staff fluctuates based upon first hand observations, staff updates, etc. The general knowledge of the subordinate commanders and staff progressively diminishes. However, with the influence of computer aided information systems and improved communications, the knowledge base climbs and remains high throughout the operation. Thus, the information gap on the battlefield diminishes proportionally with the amount of automation applied. Not only can the gap be breached on the battlefield, but also the information gap between the military and the political leadership can be narrowed as well. As the power of CNN brings the battlefield into the living rooms of the populace, so can a combined intelligence system provide information on the enemy to influence operational decisions. As the power of our technology based society increases, so, too, does the suitability of C4I for the Warrior.

The impact of technology on C4I supports the suitability of adding information systems to intelligence operations. The availability of increased data sharing can only advance the desired solution of increasing interoperability between services and allies.

Acceptability

Acceptability is a key test when addressing any course of action but especially when approaching a subject which has service-wide and international implications. The acceptability issue centers on what is acceptable to all of the services and to each of our potential allies. The evidence suggests that the services want and need a C4I for the Warrior capability. The experiences of the Gulf War demonstrateed that we are facing a revolution in the way wars are fought, and that the American serviceman and our coalition partners expect the U.S. military to use its technological superiority to win the information war as part of the military campaign.

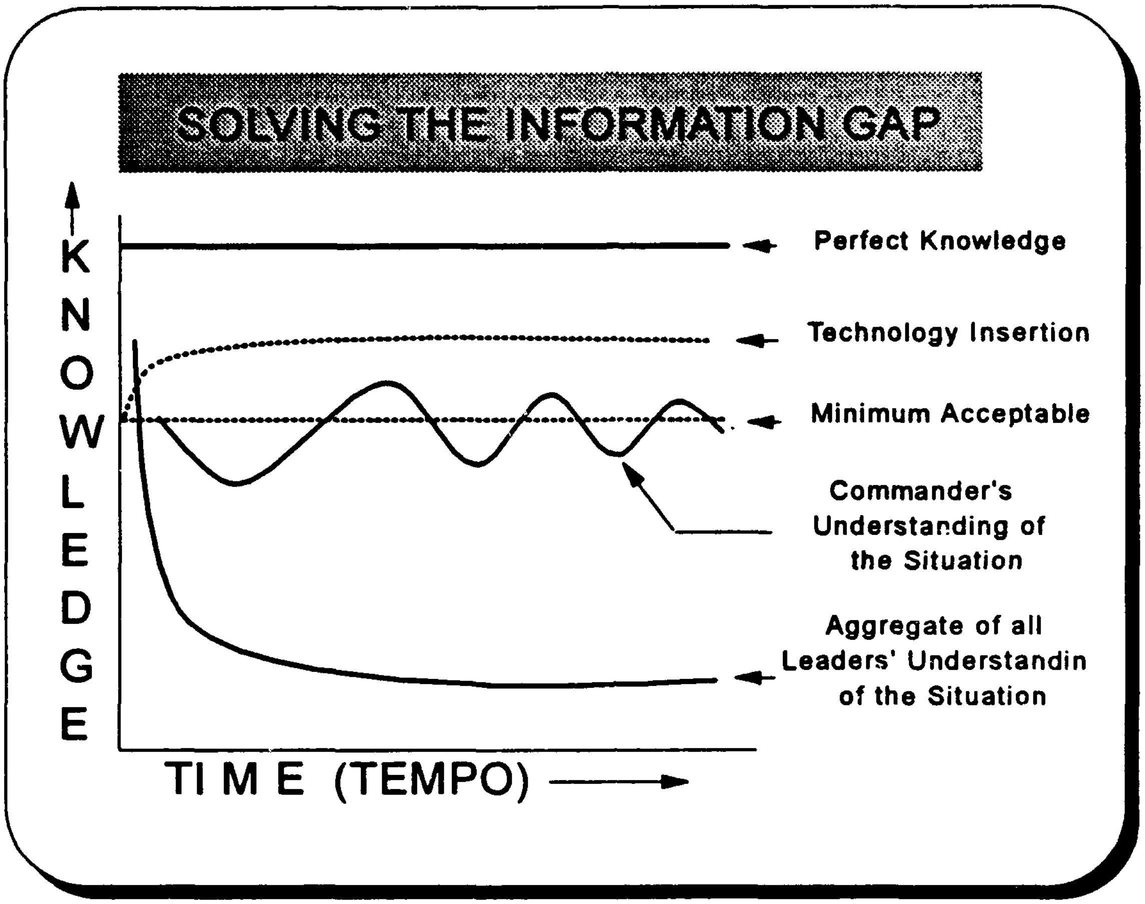


Fig. 14. Technology Impact on C4I

Source: LTG John Miller, "A View to the Future," Presentation to Signal Symposium, Ft Gordon, GA, 7 December 1993.

"War has always mirrored the progress of civilian commerce. What the world witnessed in the Gulf War is the first out break of 'third wave' warfare - a lethal twin of today's new computer-precise global economy."[73] In his book, The Third Wave , Alan Toffler describes the connection between how humans make wealth and make war. He describes "First Wave War" as that associated with the agricultural revolution. The industrial revolution launched the "Second Wave" in the making of wealth and in the making of war. Now a new basis for wealth creation is being revolutionized and the making of war is paralleling that of our economic base. Information and customized production based on intelligent technology are the basis for this Third Wave. "The rise of a knowledge based economy has been paralleled by - and accelerated - by the shift toward knowledge-based war."[74]

The relevance of Third Wave warfare to acceptability of C4I for the Warrior lies in the acceptance of the services, of our allies, and of our servicemen to recognize a fundamental change in the way we fight. It is evident that the C4I for the Warrior concept merely reflects our civilian society, and that not to accept the C4I for the Warrior concept would be less viable than moving ahead. The C4I for the Warrior concept as it applies to supporting intelligence for combined operations meets the requirements of acceptability.

Conclusions

A study of the relevant factors pertaining to intelligence fusion for combined operations reveals a number of interesting findings. **First, we have established that we have a force projection Army which will require a robust intelligence support network.** As a military which reflects our society we are increasingly dependent upon computers and information systems. From a joint perspective, we have a roadmap through the C4I for the Warrior concept to improve joint information exchange. In order to support the new force projection military that is also undergoing severe reductions in manpower, the intelligence community will depend heavily on split-based operations to reduce the forward presence of intelligence analysts, but will continue to provide all of the power of our national intelligence resources through a small contingent of analysts and briefers. Greater access to national databases and dynamic sensor data will reduce many of the manpower requirements. Future operations will have a greater reliance on HUMINT. A critical aspect and a potential weakness of the intelligence operation are that HUMINT is not surged easily nor with any degree of certainty. If HUMINT capabilities are not established in peacetime for contingencies, then we can expect relatively long lead times to establish the sources and the systems.

Secondly, we have determined that U.S. forces will most likely fight in concert with a coalition force and that the most logical place to conduct a computer interface is at the operational level of war. It is universally recognized that some coalition forces will have a greater intelligence automation capability than others and that the exchange of intelligence at the operational level will "level the playing field" as commanders conduct war in concert with allies and objectively explain the military situation to political leaders. Currently, only two theaters are considered mature, and only one of those, NATO, has an established intelligence fusion system. As the U.S. military develops computer information systems and becomes more reliant on its own information superhighway, there is an increasing threat of creating an "information gap" between the U.S. military and our potential allies. Additionally, the perception that one country in the coalition has all the intelligence capability fosters a sense that there is no need for smaller countries to provide input to the intelligence solution. A truly combined approach generates enthusiasm for all toward contributing to a complicated puzzle in which each country can provide a key element to the overall effort.

Thirdly, we have established that intelligence fusion reflects the basics of all source intelligence analysis products and that an intelligence fusion system should consist of a combination of static databases (i.e. ground order of battle, air order of battle, naval order of battle, target databases, etc.) and of dynamic databases (sensor inputs, front-line reporting, pilot reports, etc.). A multinational fusion system requires a database management concept which depends on delegated intelligence producers (accepted as experts by the coalition) and on area of interest filters (geographically defined) which allow the strategic level intelligence and the tactical level intelligence to merge and form an operational level perspective.

Finally, we have determined that our intelligence doctrine lacks a true joint perspective which impacts on a comprehensive combined doctrine. Joint Pub 2-0 is still not out in the final form and the draft version is in another rewrite phase. The test publication was weak. There was no discussion of the now accepted Joint Intelligence Centers nor any concept of how the joint intelligence staff will fit in the C4I for the Warrior concept of the future. The intelligence doctrine must be revised to support not only joint, but also combined operations to allow for the rapid creation of a functional intelligence architecture in support of contingency operations. The emerging doctrine endorses the creation of a joint intelligence facility to accomplish the intelligence functions of a joint command. Most of the CINCs have Joint Intelligence Centers but not all have included a robust intelligence fusion capability to link coalition partners.

This study concludes with a basic endorsement of the intelligence fusion concept envisioned in C4I for the Warrior and a recommendation for a combined intelligence fusion system at the operational level is included. Each theater should begin to expand [illegible] network, to include the State Department and other DoD agencies, to facilitate the further enhancement of databases. As efforts to create networks are developed, the formation of a military information superhighway will become realized. The impact of this superhighway could reach beyond the military by influencing the political and economic instruments of power through information, and thus accomplish a part of our national military strategy.

Endnotes

[1] Alan and Heidi Toffler, "War, Wealth, and a New Era in History," World Monitor, May 1991, 46.

[2] Ibid, 59.

APPENDIX A

GLOSSARY

Automatic Digital Network. A communications network used by the US DoD for worldwide computer communications.

Coalition Force. A force composed of military elements of nations that have formed a temporary alliance for some specific purpose. (Joint Pub 1-02)[1]

Communications Intelligence. Intelligence information derived from foreign communication by other than the intended recipients.

Contingency. An emergency involving military forces caused by natural disasters, terrorists, subversives, or by required military operations. Due to the uncertainty of the situation, contingencies require plans, rapid response, and special procedures to ensure the safety and readiness of personnel, installations, and equipment. (Joint Pub 1-02)[2]

Correlation Center. The hub of the LOCE network. It includes the automated processes which receive intelligence reports which have similar parametric values, store and retrieve datarecords, forward electronic mail, and route secure voice transmissions.

Enemy Situation and Correlation Element. The U.S. Air Force portion of the JTFPMO project which created ASAS.

Electronics Intelligence. Intelligence information derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear or radioactive sources.

Individual Reports Database - The portion of the LOCE database consisting of entity data records created by sensor data.

JASMIN. Joint Analysis System for Military Intelligence - An intelligence database system built by the German Ministry of Defense. Possible gateway to BICES.

Military Intelligence Integrated Data Systems. Concept developed by DIA to restructure the Automated Installation File (AIF) to enhance its operational value, and provide a centralized, composite database to address the intelligence needs of planners and operators in peace and war. MIIDS/IDB consolidates, reorganizes, and amplifies the information contained in the DIA AIF and Defense Intelligense Order of Battle System (DIOBS) files, and integrates this data with information from internal DIA asssets containing Electronic Warfare and C4I information.

North Atlantic Treaty Organization . HQ Mons, Belgium. NATO Commands are MNC (Major NATO Commands); MSC (Major Support Commands); PSC (Primary Support Commands).

National Military Strategy. The art and science of distributing and applying military power to attain national objectives in peace and war. (Approved for inclusion in the next edition of Joint Pub 1-02)[3]

National Security Strategy. The art and science of developing, applying, and coordinating the instruments of national power (diplomatic, economic, military, and informational) to achieve objectives that contribute to national strategy. (Approved for inclusion in the next edition of Joint Pub 1-02.)[4]

Standard NATO Agreement. The record of an agreement among several or all members of NATO to adopt like or similar equipment, supplies, terms and symbology; as well as operational, logistic, and administrative procedures.

TROJAN SPIRIT. A mobile intelligence system with a digital and secure voice capability utilizing satellites.

U.S. European Command. Headquartered in Stuttgart, Germany, it has command of all U.S. forces in Europe. Subordinate commands are USAREUR (US Army Europe, Heidelberg, Germany), USAFE (US Air Force Europe, Ramstein, Germany), and USNAVEUR (US Navy Europe, London, UK)

U.S. Message Text Formats. U.S. message exchange standard developed under the US Message Text Program (USMTFP).

Endnotes

[1] Joint Pub 3-0, GL5.

[2] Ibid., GL6.

[3] Ibid., GL11.

[4] Ibid., GL12.

APPENDIX B

LOCE USERS LIST

User	Location
SHAPE	Mons, Belgium
SACLANT	Norfolk, VA, USA
AFNORTH	Oslo, Norway
COMBALTAP	Karup, Denmark
COMSONOR	Stavenger, Norway
AFCENT	Brunnsum, Neatherlands
LANDCENT	Heidelberg, Germany
AIR CENT	Ramstein, Germany
AFSOUTH	Naples, Italy
LANDSOUTH	Naples, Italy
AIRSOUTH	Naples, Italy
NAVSOUTH	Naples, Italy
SRJOIC	Naples, Italy
Strike Force South	Naples, Italy
UKAIR	High Wycombe, United Kingdom
Tactical Fusion Center	Boerfink, Germany
NATO AWACS Early Warning (AEW)	Gielenkirchen, Germany
FOSIF	Rota, Spain
FAFIO	Rheindahlen, Germany
FATAC	Metz, France
ACE Mobile Force Land	Heidelberg, Germany
ACE Rapid Reaction Corps	Bielefeld, Germany
1st Belgian Corps	Koln, Germany
MOD Denmark	Copenhagen, Denmark
French 1st Army	Metz, France
1st Neatherlands Corps	Apeldoorn, Neatherlands
Royal Neatherlands Air Force	Den Haag, Neatherlands
Norwegian Intelligence Service (NIS)	Oslo, Norway
UK Defense Debriefing Team	Ashford, United Kingdom
UK Land Forces HQ	Wilton, United Kingdom
MOD United Kingdom	London, United Kingdom
Royal Navy	HMS Invinsible
USAFE	Ramstein, Germany

Ramstein Warning Office/OSC	Ramstein, Germany
USAREUR Corps Intel Ready Facility (UCIRF)	Augsberg, Germany
USAREUR, ODCSINT	Heidelberg, Germany
USEUCOM, ECJ2-O	Stuttgart, Germany
S.European Task Force(SETF)	Frankfurt, Germany
21 TAACOM	Kaiserslautern, Germany
32nd Air Defense Command	Darmstadt, Germany
16th Air Force (USAF)	Aviano, Italy
5th ATAF	Vincenza, Italy
Computer Systems Iternational (CSI)	California, USA
JAC LOCE Division (DOL)	Molesworth, United Kingdom
JAC OB Division (DOBE)	Molesworth, United Kingdom
JAC Operations Center	Molesworth, United Kingdom
JAC Yugo Working Group	Molesworth, United Kingdom
JTF- PROVIDE PROMISE	Naples, Italy
JTF- PROVIDE PROMISE (FWD)	Zagreb, Croatia
COMBRITFOR	Split, Croatia
COAC Fwd	Kiseljac, Bosnia-Hertzegovenia

BIBLIOGRAPHY

BOOKS

Campen, Alan D. The First Information War. Fairfax, V.A. : AFCEA International Press, 1992.

Cushman, John H. Command and Control of Theater Forces: Adequacy. Washington, D.C.: AFCEA International Press, 1985.99

McKnight, Clarence E., ed. Control of Joint Forces: A New Perspective. Fairfax, Va.: AFCEA International Press, 1989.

Boyles, Jon L., ed. Issues in C3I Program Management. Washington, D.C. : AFCEA International Press, 1985.

GOVERNMENT DOCUMENTS

The White House. United States of America National Security Strategy. Washington, D.C.: U.S. GPO, 1993.

U.S. Army. Department of the Army Memorandum. "Operational Requirements Document (ORD) for the All Source Analysis System." Washington, D.C., August 1993.

________. Office of the Deputy Chief of Staff for Operations and Plans, State of America's Army. Washington, D.C.: U.S. GPO, 1993.

________. FM 34-1. Intelligence and Electronic Warfare Operations. Washington, D.C.: U.S. GPO, 1987.

________. FM 34-3. Intelligence Analysis. Washington, D.C.: U.S. GPO, 1990.

________ . FM 100-5. Operations. Washington, D.C.: U.S. GPO, 1993.

________ . FM 100-8. Combined Army Operations (Preliminary Draft). Washington, D.C.: U.S. GPO, 1992.

________ . DOD Directive 2010.6. "Standardization and Interoperability of Weapon Systems and Equipment within the North Atlantic Treaty Organization (NATO)." Washington, D.C.: U.S. GPO, March 05, 1980.

________ . DOD Directive 4630.5 "Compatibility and Interoperability of Tactical Command, Control and Communications, and Intelligence Systems." Washington, D.C.: U.S. GPO, October 1985.

________. Command and General Staff College C510. Joint and Combined Environments. Ft Leavenworth, K.S.: U.S. GPO, August 1993.

________ . Office of the Deputy Chief of Staff for Operations and Plans. State of America's Army .Washington, D.C.: U.S. GPO, 1993.

USEUCOM PAM. Joint Tactical Fusion - Limited Operational Capability Europe. Stuttgart, Germany: GPO, 1985.

USEUCOM. Joint Analysis Center, LOCE Division. "Linked Operations Intelligence Centers Europe." RAF Molesworth, UK, 1993.

________ . Linked Ops-Intel Centers Europe Program Management Office. Linked Ops-Intel Centers Europe Workstation Manual. Arlington, VA, June 1993.

U.S Joint Chiefs of Staff. JCS Pub 0-1, Basic National Defense Doctrine. Washington, D.C.: U.S. GPO, 1991.

________ . Joint Pub 2-0 (Test Pub), Doctrine for Intelligence Support to Joint Operations . Washington, D.C.: U.S. GPO, 1991.

________ . JCS Memorandum of Policy 160. "Compatibility and Interoperability of Tactical Command, Control, Communications and Intelligence Systems. Washington,D.C.: U.S. GPO. Issued May 3, 1967, 3rd Revision Issued January 7, 1986.

________ . JULLS Report Number 12142-94679 (00108). Integration of Coalition Forces/Intelligence. Submitted by G2, 10th Mtn Div, LTC Joyce, 22 Mar 1993.

________ . JULLS Report Number 10834-01832 (00104). Trojan Priorities and Requirements . Submitted by G2, 10th Mtn Div, LTC Joyce, 22 Mar 1993.

________. National Military Strategy of the United States. Washington, D.C.: U.S. GPO, January 1992.

PERIODICALS AND ARTICLES

Armstrong, Richard LT COL. "Graphic INTSUM." Military Intelligence (March 1987). 11-14.

Gordon, Don. "The JTIDS/PLRS hybrid - a NATO standard?" Military Technology XI (May 1987): 97-106.

Greenwood, Ted and Lohnson, Stewart. "NATO Force Plannng Without the Soviet Threat." Command and General Staff College, C320 Syllabus. Corps and Division Operations. (August 1993).

Gust, David R. "Army Battlefield C3I Using Satellite Communications." Signal (May 1989): 57-59.

Kulda, Nancy R. "Artificial Intelligence and C3I analysis and reporting." Signal 41 (April 1987): 53-57.

Marcus, Daniel J. "NATO Plans Major Review of Intelligence System." Army Times (29 February 1988):34.

Meier, A.L. "BICES: a Central Region perspective" International Defense Review 10 (October 1986): 1445-1449.

Pengelley, Rupert. "HEROS and Wavell battlefield ADP enters a new era." International Defense Review 10 (October 1986): 1459-1464.

Recter, R.J. "ATCCS: An Integrated C3 Environment." Signal 43 (June 1989): 181-188.

Robinson, Clarence A. "Army's digital devices move presses tactical automation." Signal 45 (Nov 1990): 23-32.

Seiffert, Siegfried. "Technical Interoperability of the command, control and information system in the Central Region." Military Technology XI (May 1987): 92-95.

Stewart, John F. Jr. "Desert Storm: A 3d Army Perspective." Military Intelligence (October - December 1991): 22-23.

OTHER SOURCES

"Army Weaponry and Equipment." Army Green Book 42 (October 1992): 287.

"Intelligence and Electronic Warfare (IEW) System Fact Sheets," (Ft Huachuca, AZ, 1993) 45.

Joint Defense Intelligence Support Services Program Management Office Pamphlet. "Joint Defense Intelligence Support Services." Suitland, MD (1993).

Joint Chief of Staff Pamphlet."C4I for The Warrior." Washington, D.C.: U.S. GPO, 1992.

Joint Chief of Staff Pamphlet."C4I for The Warrior." Washington, D.C.: U.S. GPO, 1993.

Maynard, Bob, COL, USA. "An Integrated Set of Common Software Applications." JDISS Program Management Office briefing. Suitland, Md, 1993.

Miller, John A. LTG, USA. "A View to the Future," Presentation to Signal Symposium, Ft Gordon, GA, 7 December 1993.

Roques, P.F. "Operational Decisions and the Information Explosion. What are the Critical Joint Warfighting Requirements for the CINC (Commander in Chief)." Study Project. U.S. Army War College, Carlisle Barracks, PA, 1989.

Sirah, H.C. "Operational Aspects of Desert Shield and Desert Storm." Study Project. Army War College. Carlisle Barracks, PA. 1992.

Stewart, John F., Jr. "MI Corps Intelligence Strategy - Intelligence in Force Projection." Briefing to CGSC intelligence officers, 4 August 1993, Ft Leavenworth, KS.

"Standard Theater Army Command and Control." PEO, Command and Control Systems Pamphlet. Ft Monmouth, N.J.: U.S. GPO, 1993.

Wickam, W.E. "Institutionalizing Operational Intelligence in the Joint Environment." Final Report. Naval War College. Newport, RI, 1992.

Zinni, Antony C. , USMC. Address to the CGSC class on his view of Somalia. 30 November 1993, Ft Leavenworth, KS.

INITIAL DISTRIBUTION LIST

1. Combined Arms Research Library
U.S. Army Command and General Staff College
Fort Leavenworth, Kansas 66027-6900

2. Defense Technical Information Center
Cameron Station
Alexandria, Virginia 22314

3. Lt Col Michael E. Barrington
Department of Joint and Combined Operations
USACGSC
Fort Leavenworth, Kansas 66027-6900

4. LTC Kathleen R. Sower
The Center for Army Tactics
USACGSC
Fort Leavenworth, Kansas 66027-6900

5. LTC Ernest M. Pitt, Jr.
207 16th St.
500 Price Bldg.
Ashland, Kentucky 41101

CERTIFICATION FOR MMAS DISTRIBUTION STATEMENT

1. Certification Date: 05/ 05 / 94

2. Thesis Author: MAJOR John P. Ritchey II

3. Thesis Title: Intelligence Fusion for Combined Operations

4. Thesis Committee Members Signatures: Michael E. [illegible]

Kathleen R. [illegible]

5. Distribution Statement: See distribution statements A-X on reverse, then circle appropriate distribution statement letter code below:

[✓ A] B C D E F X SEE EXPLANATION OF CODES ON REVERSE

If your thesis does not fit into any of the above categories or is classified, you must coordinate with the classified section at CARL.

6. Justification: Justification is required for any distribution other than described in Distribution Statement A. All or part of a thesis may justify distribution limitation. See limitation justification statements 1-10 on reverse, then list, below, the statement(s) that applies (apply) to your thesis and corresponding chapters/sections and pages. Follow sample format shown below:

S--------SAMPLE--------------SAMPLE-----------------SAMPLE------------S

A	Limitation Justification Statement /	Chapter/Section /	Page(s)	A
M				M
P	Direct Military Support (10) /	Chapter 3 /	12	P
L	Critical Technology (3) /	Sect. 4 /	31	L
E	Administrative Operational Use (7) /	Chapter 2 /	13-32	E

---------SAMPLE--------------SAMPLE-----------------SAMPLE------------

Fill in limitation justification for your thesis below:

Limitation Justification Statement Chapter/Section Page(s)

/ /

/ /

/ /

/ /

/ /

7. MMAS Thesis Author's Signature:

STATEMENT A: Approved for public release; distribution is unlimited. (Documents with this statement may be made available or sold to the general public and foreign nationals).

STATEMENT B: Distribution authorized to U.S. Government agencies only (insert reason and date ON REVERSE OF THIS FORM). Currently used reasons for imposing this statement include the following:

1. Foreign Government Information. Protection of foreign information.

2. Proprietary Information. Protection of proprietary information not owned by the U.S. Government.

3. Critical Technology. Protection and control of critical technology including technical data with potential military application.

4. Test and Evaluation. Protection of test and evaluation of commercial production or military hardware.

5. Contractor Performance Evaluation. Protection of information involving contractor performance evaluation.

6. Premature Dissemination. Protection of information involving systems or hardware from premature dissemination.

7. Administrative/Operational Use. Protection of information restricted to official use or for administrative or operational purposes.

8. Software Documentation. Protection of software documentation - release only in accordance with the provisions of DoD Instruction 7930.2.

9. Specific Authority. Protection of information required by a specific authority.

10. Direct Military Support. To protect export-controlled technical data of such military significance that release for purposes other than direct support of DoD-approved activities may jeopardize a U.S. military advantage.

STATEMENT C: Distribution authorized to U.S. Government agencies and their contractors: (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT D: Distribution authorized to DoD and U.S. DoD contractors only; (REASON AND DATE). Currently most used reasons are 1, 3, 7, 8, and 9 above.

STATEMENT E: Distribution authorized to DoD only; (REASON AND DATE). Currently most used reasons are 1, 2, 3, 4, 5, 6, 7, 8, 9, and 10.

STATEMENT F: Further dissemination only as directed by (controlling DoD office and date), or higher DoD authority. Used when the DoD originator determines that information is subject to special dissemination limitation specified by paragraph 4-505, DoD 5200.1-R.

STATEMENT X: Distribution authorized to U.S. Government agencies and private individuals of enterprises eligible to obtain export-controlled technical data in accordance with DoD Directive 5230.25; (date). Controlling DoD office is (insert).